(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2001143009 A

(43) Date of publication of application: 25.05.01

(51) Int. Cl G06F 19/00
G06F 12/14
G09C 1/00
G11B 20/10
H04L 9/10

(21) Application number: 2000038875

(22) Date of filing: 16.02.00

(30) Priority: 17.02.99 JP 11039080
01.09.99 JP 11247457

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

(72) Inventor: TERADA MASAYUKI
FUJIMURA TAKASHI
KUNO HIROSHI
KAKAN KURAYUKI

(54) METHOD, SYSTEM AND DEVICE FOR CIRCULATING ORIGINAL DATA AND RECORDING MEDIUM WITH ORIGINAL DATA CIRCULATION PROGRAM RECORDED THEREON

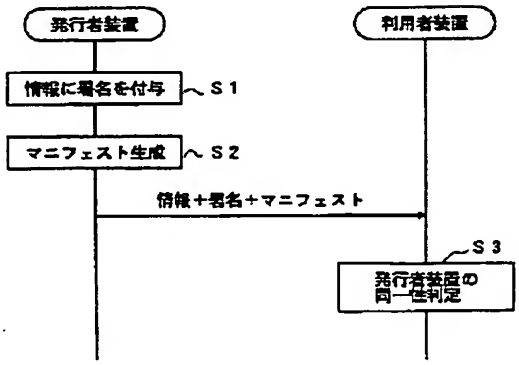
(57) Abstract:

PROBLEM TO BE SOLVED: To provide an original data circulation system for reducing processing loads, such as processing speed and storage capacity.

SOLUTION: This system is provided with an issuer device having a means for generating original information having 1st information, corresponding to the issuer device and 2nd information which corresponds to data and transferring the generated information, a means for verifying the validity of a transfer source device for the original information when the original information is transferred from another device, a user device having a means for storing the original information when the validity is certified, a means for verifying the validity of the original information transfer source information when the original information is transferred from the user device, and a ticket examiner device having a data processing means for executing data processing corresponding to the 2nd information, when the validity is certified.

COPYRIGHT: (C)2001,JPO

本発明の第1の実施例における原理を説明するための図



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－143009
（P2001－143009A）
(43)公開日　平成13年５月25日(2001.5.25)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　12/14	３１０Ｚ	５Ｂ０１７
12/14	３１０	Ｇ０９Ｃ　1/00	６４０Ａ	５Ｂ０５５
Ｇ０９Ｃ　1/00	６４０	Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｇ０６Ｆ　15/30	Ｚ	５Ｊ１０４
Ｈ０４Ｌ　9/10			Ｌ	９Ａ００１

審査請求　有　請求項の数71　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願2000－38875(P2000－38875)
(22)出願日　平成12年２月16日(2000.2.16)
(31)優先権主張番号　特願平11－39080
(32)優先日　平成11年２月17日(1999.2.17)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－247457
(32)優先日　平成11年９月１日(1999.9.1)
(33)優先権主張国　日本（ＪＰ）

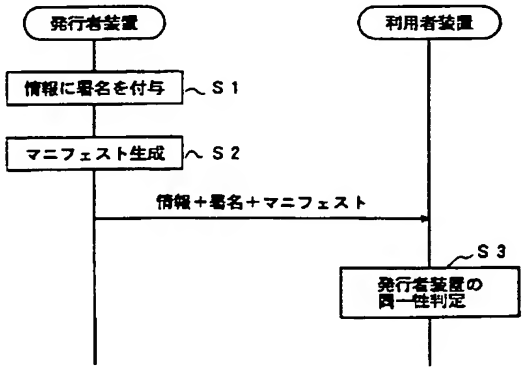
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　寺田　雅之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　藤村　考
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　原本データ流通方法、原本データ流通システム及び装置、並びに原本データ流通プログラムを記録した記録媒体

(57)【要約】
【課題】処理速度や記憶容量等の処理負荷を低減させる原本データ流通システムを提供する。
【解決手段】発行者装置に対応する情報を第１の情報とデータに対応する第２の情報とを有する原本性情報を生成し、転送する手段を有する発行者装置と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に該原本性情報を格納する手段とを有する利用者装置と、利用者装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に第２の情報に対応するデータに対する処理を行うデータ処理手段とを有する改札者装置とを有する。

本発明の第１の実施例における原理を説明するための図



1

【特許請求の範囲】

【請求項１】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、
データを発行する発行者装置に対応する第１の情報を生成する手段と、該第１の情報を転送する手段と、データに対応する第２の情報を転送する手段とを有する装置と、
受信した第１の情報の有効性を判定する手段と、有効な第１の情報に対応する発行者装置が正当なものであるかどうかを検証し、正当である場合に前記第２の情報に対応するデータを有効と判定する手段とを有する装置とを有することを特徴とする原本データ流通システム。

【請求項２】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける原本データ流通方法であって、
データを発行する発行者装置に対応する第１の情報を生成し、
データに対応する第２の情報を転送し、
前記第１の情報を転送し、
受信した第１の情報の有効性を判定し、
有効な第１の情報に対応する発行者装置が正当なものであるかどうかを検証し、
正当である場合に前記第２の情報に対応するデータを有効と判定する原本データ流通方法。

【請求項３】　価値を有する電子的な情報の蓄積を行うデータ蓄積方法において、
電子的な情報の発行者装置による該電子的な情報に対する署名である第１の情報を付与するステップと、
前記発行者装置により前記第１の情報が付与された電子的な情報と対応する第４の情報を生成するステップと、
電子的な情報利用装置において、前記第１の情報と前記第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するステップとを有することを特徴とするデータ蓄積方法。

【請求項４】　電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するステップと、
前記情報利用装置において、前記検証鍵からセッション情報を生成するステップと、
前記セッション情報の正当性を判定するステップとを有する請求項３記載のデータ蓄積方法。

【請求項５】　前記第２の情報の格納と、署名者の同一性の判定とを、耐タンパ装置を用いて行うステップを有する請求項３記載のデータ蓄積方法。

【請求項６】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、
電子的な情報に第１の情報を付与し、該電子的な情報と対応するマニフェストの第２の情報を生成する発行者装置と、
前記第１の情報と前記第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する利用者装置とを有することを特徴とするデータ蓄積システム。

2

【請求項７】　前記利用者装置は、
電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得する手段を有し、
前記検証鍵からセッション情報を生成する手段と、
前記セッション情報の正当性を判定する手段を有する改札装置を更に有する請求項６に記載のデータ蓄積システム。

【請求項８】　前記利用者装置は、
前記第２の情報を耐タンパ性の装置に格納し、前記発行者装置の同一性を判定する手段を含む請求項６記載のデータ蓄積システム。

【請求項９】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を利用する利用者装置であって、
署名が付与された電子的な情報の格納及び抽出を行うための第１の格納手段と、
前記電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、
該マニフェストが正当であるかどうかを検証する第１の認証手段と、
該マニフェストが正当であることが前記第１の認証手段により検証された時のみ、該マニフェストを前記第２の格納手段に格納する第１の制御手段とを有することを特徴とする利用者装置。

【請求項１０】　前記第２の格納手段及び前記第１の認証手段は、耐タンパ性を有する請求項９記載の利用者装置。

【請求項１１】　前記第１の認証手段は、
前記第１の格納手段に格納された前記署名が付与された情報の有効性を、該情報と対応するマニフェストが前記第２の格納手段に格納されているか否かにより検証し、該マニフェストが該第２の格納手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第２の格納手段に格納されていなかったときには、該情報を無効とする手段を含む請求項９記載の利用者装置。

【請求項１２】　情報に署名を付与する署名手段と、
マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記電子的な情報の署名者とが同一であることを検証する第２の認証手段と、
ある電子的な情報に対応するマニフェストを前記第２の格納手段から他の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、前記署名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第２の認証手段により検証し、検証に成功した時のみ前記他の格納手段に該マニフェストを格納する第２の制御手段と

を含む請求項９に記載の利用者装置。

【請求項１３】　前記利用者装置は、システム内で一意性を持つセッション情報を生成するセッション情報生成手段を含み、

該セッション情報は、該利用者装置の検証鍵と連番からなり、該利用者装置に保持されるとともに、マニフェストの送信側に送られ、

該利用者装置は、該送信側から該マニフェストとともに該セッション情報を受信し、該セッション情報の正当性を前記保持したセッション情報を用いて行うことによりマニフェストの複製を防止する請求項９に記載の利用者装置。

【請求項１４】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を発行する発行者装置であって、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

該電子的な情報及び該信任情報に署名を付与する署名手段と、

マニフェストを生成するマニフェスト生成手段と、

該電子的な情報及び該信任情報を利用者装置に送信する手段と、

該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信する手段と、

該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信する手段とを有することを特徴とする発行者装置。

【請求項１５】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報の権利を行使する対象である改札者装置であって、

利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信する手段と、

システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信する手段と、

該利用者装置からマニフェストと該セッション情報を含む情報を受信する手段と、

該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証する手段を有することを特徴とする改札者装置。

【請求項１６】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

該データ蓄積システムは、電子的な情報を利用する利用者装置と、電子的な情報を発行する発行者装置と、電子的な情報の権利を行使する対象である改札者装置とを有し、

前記利用者装置は、

署名が付与された電子的な情報の格納及び抽出を行うための第１の格納手段と、

前記電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、

該マニフェストが正当であるかどうかを検証する認証手段と、

該マニフェストが正当であることが前記認証手段により検証された時のみ、該マニフェストを前記第２の格納手段に格納する第１の制御手段とを有し、

前記発行者装置は、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

該電子的な情報及び該信任情報に署名を付与する署名手段と、

マニフェストを生成するマニフェスト生成手段と、

該電子的な情報及び該信任情報を利用者装置に送信する手段と、

該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信する手段と、

該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信する手段とを有し、

前記改札者装置は、

利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信する手段と、

システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信する手段と、

該利用者装置からマニフェストと該セッション情報を含む情報を受信する手段と、

該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証する手段とをを有することを特徴とするデータ蓄積システム。

【請求項１７】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報に署名した第１の情報を付与し、該電子的な情報と対応するマニフェストの第２の情報を生成して、前記第１の情報に付与するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項１８】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

前記第１の情報と前記第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項１９】　電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するプロセスと、

前記検証鍵からセッション情報を生成するプロセスと、

前記セッション情報の正当性を判定するプロセスを含む

請求項１８記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項２０】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、
署名が付与された情報を第１の記憶手段に格納すると共に、抽出を行うための第１の格納プロセスと、
前記電子的な情報と１対１に対応するマニフェストを第２の記憶手段に格納すると共に、抽出を行うための第２の格納プロセスと、
該マニフェストが正当であるかどうかを検証する第１の認証プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項２１】　前記第１の認証プロセスは、
前記第１の記憶手段に格納された前記署名が付与された情報の有効性を、該情報と対応するマニフェストが前記第２の記憶手段に格納されているか否かにより検証し、
該マニフェストが該第２の記憶手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第２の記憶手段に格納されていなかったときには、該情報を無効とするプロセスを含む請求項２０記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項２２】　情報に署名を付与するための署名プロセスと、
マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第２の認証プロセスとある電子的な情報に対応するマニフェストを移動させる際に、該マニフェストを抽出し、前記署名プロセスにより該マニフェストに署名を付与し、該第２の格納プロセスから該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第２の認証プロセスにより検証し、検証に成功した時のみ該マニフェストを移動するプロセスとを含む請求項２０記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項２３】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、
前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成プロセスと、
該電子的な情報及び該信任情報に署名を付与する署名プロセスと、
マニフェストを生成するマニフェスト生成プロセスと、
該電子的な情報及び該信任情報を利用者装置に送信するプロセスと、
該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信するプロセスと、
該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信するプロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項２４】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける改札装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、
利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信するプロセスと、
システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信するプロセスと、
該利用者装置からマニフェストと該セッション情報を含む情報を受信するプロセスと、
該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項２５】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける原本データ流通方法であって、
第１の装置が、ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送する転送ステップと、
第２の装置が前記原本性情報の転送元装置を検証し、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証ステップと、
該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該第２の装置が該原本性情報を有効であると判別する第２の認証ステップとを有することを特徴とする原本データ流通方法。

【請求項２６】　前記第１の装置が秘密鍵を秘匿するステップと、
前記第２の装置が１乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手するステップとを更に有し、
前記第１の認証ステップは、
転送元の前記第１の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証するステップを有する請求項２５記載の原本データ流通方法。

【請求項２７】　前記転送ステップは、
自装置が１乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を前記第２の装置に転送するステップを有し、
前記原本データ流通方法は、前記第２の装置が１乃至複数の第三者に対応する第三者情報を保持、または、入手するステップを有し、

前記第１の認証ステップは、
転送元装置である前記第１の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第１の装置を認証するステップを有する請求項２５記載の原本データ流通方法。

【請求項２８】　前記原本データ流通方法は、前記第２の装置が前記第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するステップを有し、
前記第１の認証ステップは、
原本性情報の転送元である前記第１の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第１の情報から、保持されている前記第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するステップを有する請求項２７記載の原本データ流通方法。

【請求項２９】　前記原本データ流通方法は、前記第２の装置が前記第１の情報と前記第２の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手するステップを有し、
前記第１の認証ステップは、
転送された前記原本性情報の前記第１の情報と前記第２の情報から、前記第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するステップを有する請求項２７記載の原本データ流通方法。

【請求項３０】　前記原本データ流通方法は、
前記第１の装置が秘密鍵を秘匿し、前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第２の装置に転送するステップと、
前記第２の装置が前記公開鍵証明書を検証して署名者の公開鍵を特定し、１乃至複数のフィガープリントを保持または、入手するステップとを更に有し、
前記第１の認証ステップは、
前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第１の装置を認証するステップを有する請求項２５記載の原本データ流通方法。

【請求項３１】　前記原本データ流通方法は、
前記第２の装置が、前記第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するステップを有し、
前記第１の認証ステップは、
転送された前記原本性情報の第１の情報から、保持されている前記利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するステップを有する請求項２５記載の原本データ流通方法。

【請求項３２】　前記原本データ流通方法は、
前記第２の装置が、前記第１の情報と前記第２の情報から、１乃至複数の前記第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するステップを有し、
前記第１の認証ステップは、
転送された前記原本性情報の第１の情報と第２の情報とから、保持されている前記利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するステップを有する請求項２５記載の原本データ流通方法。

【請求項３３】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、
ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送する転送手段を有する第１の装置と、
前記原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証手段と、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証手段とを有する第２の装置とを有することを特徴とする原本データ流通システム。

【請求項３４】　前記第１の装置は、
秘密鍵を秘匿する手段を更に有し、
前記第２の装置は、
１乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手する手段を更に有し、
前記第２の装置の前記第１の認証手段は、
転送元の前記第１の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証する請求項３３記載の原本データ流通システム。

【請求項３５】　前記第１の装置の前記転送手段は、
自装置が１乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応

する情報である第三者証明を前記第２の装置に転送する手段を有し、

前記第２の装置は、

１乃至複数の第三者に対応する第三者情報を保持、または、入手する手段を有し、

前記第１の認証手段は、

転送元装置である前記第１の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第１の装置を認証する請求項３３記載の原本データ流通システム。

【請求項３６】　前記第２の装置は、

前記第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

原本性情報の転送元である前記第１の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第１の情報から、保持されている前記第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証する請求項３５記載の原本データ流通システム。

【請求項３７】　前記第２の装置は、

前記第１の情報と前記第２の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

転送された前記原本性情報の前記第１の情報と前記第２の情報から、前記第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証する請求項３５記載の原本データ流通システム。

【請求項３８】　前記第１の装置は、

秘密鍵を秘匿する手段と、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第２の装置に転送する手段を有し、

前記第２の装置は、

前記公開鍵証明書を検証して署名者の公開鍵を特定する手段と、

１乃至複数のフィガープリントを保持または、入手する手段とを更に有し、

前記第１の認証手段は、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第１の装置を認証する請求項３３記載の原本データ流通システム。

【請求項３９】　前記第２の装置は、

前記第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

転送された前記原本性情報の第１の情報から、保持されている前記利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証する請求項３３記載の原本データ流通システム。

【請求項４０】　前記第２の装置は、

前記第１の情報と前記第２の情報から、１乃至複数の前記第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

転送された前記原本性情報の第１の情報と第２の情報とから、保持されている前記利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証する請求項３３記載の原本データ流通システム。

【請求項４１】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける発行者装置であって、

自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する原本性情報生成手段と、前記原本性情報を転送する原本性情報転送手段とを有する発行者装置を有することを特徴とする発行者装置。

【請求項４２】　秘密鍵を秘匿する手段と、

前記秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを前記第１の情報として生成する手段を有する請求項４１記載の発行者装置。

【請求項４３】　前記原本性情報の前記第２の情報として、データの一方向関数による出力を生成する手段を有する請求項４１記載の発行者装置。

【請求項４４】　前記原本性情報の前記第２の情報として、ネットワーク上の資源の識別子を用いる請求項４３記載の発行者装置。

【請求項４５】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける利用者装置であって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原

本性情報を転送する原本性情報転送手段と、
他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、
前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、
前記認証手段で前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有することを特徴とする利用者装置。

【請求項４６】　自装置から前記原本性情報を転送する際に、該原本性情報を消去する手段を有する請求項４５記載の利用者装置。

【請求項４７】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける改札者装置であって、
原本性情報の転送元装置を特定する特定手段と、
前記転送元装置を認証する認証手段と、
前記認証手段において、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対応する処理を行うデータ処理手段を有することを特徴とする改札者装置。

【請求項４８】　発行者装置に対応する情報である発行者情報を保持もしくは、入手する手段を更に有し、
前記データ処理手段は、
前記認証手段において、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第１の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第２の情報に対応するデータに対する処理を行う請求項４７記載の改札者装置。

【請求項４９】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、
発行者装置に対応する情報を第１の情報とデータに対応する第２の情報とを有する原本性情報を生成し、転送する手段を有する発行者装置と、
他の装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に該原本性情報を格納する手段とを有する利用者装置と、
利用者装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に第２の情報に対応するデータに対する処理を行うデータ処理手段とを有する改札者装置と、
を有することを特徴とする原本データ流通システム。

【請求項５０】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、
自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成手段と、該原本性情報を転送する第１の原本性情報転送手段とを有する発行者装置と、
ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する第２の原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証手段と、該第１の認証手段で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置と、
原本性情報の転送元装置を特定する第２の特定手段と、前記転送元装置を認証する第２の認証手段と、該第２の認証手段において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理手段を有する改札者装置とを有することを特徴とする原本データ流通システム。

【請求項５１】　前記改札者装置は更に、
利用者装置から転送された原本性情報を発行者装置に転送する手段を有し、
前記発行者装置は更に、
該原本性情報が該発行者装置の生成したものであるかどうかを検証する手段と、
該原本性情報が正当な流通経路を介して転送されたものであるかどうかを検証する手段と、
前記第２の情報に対応するデータに対する処理が行われたかどうかを検証する手段と、
該データに応じた価値を前記改札者装置に提供する手段と、を有する請求項４９に記載の原本性データ流通システム。

【請求項５２】　前記発行者装置は、
前記データの使用可能回数を度数情報として前記原本性情報に加える手段を更に有し、
前記利用者装置及び前記改札者装置は、それぞれ該度数情報を検証する手段を更に有し、
該利用者装置は、該データを該使用可能回数だけ使用可能である請求項４９に記載の原本性データ流通システム。

【請求項５３】　前記原本データ流通システムにおける装置が原本性情報を転送する際には、前記原本性データ流通システム内で一意性を持つセッション情報を共に転送し、
原本性情報を転送する送信側装置は該原本性情報及びセッション情報を保持しておき、

受信側の装置は、該原本性情報を受信すると、該セッション情報を送信側装置に転送し、
該送信側装置は、該原本性情報及び該セッション情報を削除する請求項４９に記載の原本データ流通システム。
【請求項５４】　前記利用者装置は更に、前記原本性情報を生成する手段を有する請求項４９に記載の原本性データ流通システム。
【請求項５５】　電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、
第１の装置に搭載される、
ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送させる転送プロセスと、
第２の装置に搭載される、
前記原本性情報の転送元装置を特定する特定プロセスと、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証プロセスと、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。
【請求項５６】　前記第１の装置に搭載される、秘密鍵を秘匿するプロセスを更に有し、
前記第２の装置に搭載される、
１乃至、複数の秘密鍵に対応する公開鍵の一方向性関数による出力である自装置のフィンガープリントを保持、または、入手するプロセスを更に有し、
前記第１の認証プロセスは、
転送元の前記第１の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項５５記載の原本データ流通プログラムを格納した記憶媒体。
【請求項５７】　前記第１の装置に搭載されるの前記転送プロセスは、
自装置が１乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を前記第２の装置に転送するプロセスを有し、
前記第２の装置に搭載される、
１乃至複数の第三者に対応する第三者情報を保持、または、入手するプロセスを有し、
前記第２の装置に搭載される前記第１の認証プロセスは、
転送元装置である前記第１の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第１の装置を認証するプロセスを含む請求項５５記載の原本データ流通プログラムを格納した記憶媒体。
【請求項５８】　前記第２の装置に搭載される、
前記第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するプロセスを有し、
前記第１の認証プロセスは、
原本性情報の転送元である前記第１の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第１の情報から、保持されている前記第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項５７記載の原本データ流通プログラムを格納した記憶媒体。
【請求項５９】　前記第２の装置に搭載される、
前記第１の情報と前記第２の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手するプロセスを有し、
前記第１の認証プロセスは、
転送された前記原本性情報の前記第１の情報と前記第２の情報から、前記第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項５７記載の原本データ流通プログラムを格納した記憶媒体。
【請求項６０】　前記第１の装置に搭載される、
秘密鍵を秘匿するプロセスと、
前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第２の装置に転送するプロセスを有し、前記第２の装置に搭載される、
前記公開鍵証明書を検証して署名者の公開鍵を特定するプロセスと、
１乃至複数のフィガープリントを保持または、入手するプロセスとを更に有し、
前記第１の認証プロセスは、
前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第１の装置を認証するプロセスを含む請求項５５記載の原本データ流通プログラムを格納した記憶媒体。
【請求項６１】　前記第２の装置に搭載される、
前記第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第１の認証プロセスは、
転送された前記原本性情報の第１の情報から、保持されている前記利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項５５記載の原本データ流通プログラムを格納した記憶媒体。

【請求項６２】　前記第２の装置に搭載される、
前記第１の情報と前記第２の情報から、１乃至複数の前記第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、
前記第１の認証プロセスは、
転送された前記原本性情報の第１の情報と第２の情報とから、保持されている前記利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項５５記載の原本データ流通プログラムを格納した記憶媒体。

【請求項６３】　電子的な情報である原本データの蓄積や流通を行う発行者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、
前記発行者装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する原本性情報生成プロセスと、
前記原本性情報を転送する原本性情報転送プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項６４】　秘密鍵を秘匿するプロセスと、
前記秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを前記第１の情報として生成するプロセスを有する請求項６３記載の原本データ流通プログラムを格納した記憶媒体。

【請求項６５】　前記原本性情報の前記第２の情報として、データの一方向関数による出力を生成するプロセスを有する請求項６３記載の原本データ流通プログラムを格納した記憶媒体。

【請求項６６】　前記原本性情報の前記第２の情報として、ネットワーク上の資源の識別子を用いるプロセスを含む請求項６５記載の原本データ流通プログラムを格納した記憶媒体。

【請求項６７】　電子的な情報である原本データの蓄積や流通を行う利用者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、
ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する原本性情報転送プロセスと、
他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定プロセスと、
前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証プロセスと、
前記認証プロセスで前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項６８】　前記利用者装置から前記原本性情報を転送する際に、該原本性情報を消去するプロセスを有する請求項６７記載の原本データ流通プログラムを格納した記憶媒体。

【請求項６９】　電子的な情報である原本データの蓄積や流通を行う改札者装置に搭載される原本データ流通プログラムであって、
原本性情報の転送元装置を特定する特定プロセスと、
前記転送元装置を認証する認証プロセスと、
前記認証プロセスにおいて、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対応する処理を行うデータ処理プロセスを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項７０】　発行者装置に対応する情報である発行者情報を保持もしくは、入手するプロセスを更に有し、
前記データ処理プロセスは、
前記認証プロセスにおいて、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第１の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第２の情報に対応するデータに対する処理を行う請求項６９記載の原本データ流通プログラムを格納した記憶媒体。

【請求項７１】　電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、
発行者装置に搭載される、
前記発行者装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成プロセスと、
前記原本性情報を転送する第１の原本性情報転送プロセスと、
利用者装置に搭載される、
ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する第２の原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定プロセスと、
前記転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証プロセスと、
前記第１の認証プロセスで該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスと、
改札者装置に搭載される、
原本性情報の転送元装置を特定する第２の特定プロセスと、
前記転送元装置を認証する第２の認証プロセスと、
前記第２の認証プロセスにおいて、前記改札者装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体に係り、特に、電子チケットなどの権利を表象するデータやディジタル著作物など、有効な複製数を一定数以下に保つことが必要とされるデータについて、蓄積や配送のための手段を提供するための原本データ流通方法、原本データ流通システム及び装置、並びに原本データ流通プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】権利を表象したデータや著作物などは、配布者などの意図する数を越えて同時に複製が存在することを防止することが求められる。即ち、配布したデータが利用者などにより複製され、それらが多重に利用されることを防ぐ必要がある。

【０００３】従来は、以下で示すような技術によりそのような多重利用を防止している。

【０００４】第１の方法として、権利を表象するデータについて、権利の提供者などにより、当該データの使用履歴を保持しておき、権利の行使時に、当該データが既に使用されていないかどうかを検証する。もし、既に使用されていれば、当該データが表象する権利の行使を拒否する。

【０００５】第２の方法として、データ自身を耐タンパ装置に格納し、当該データを当該耐タンパ装置以外からは参照できないようにする。権利の行使時には、当該データを該耐タンパ装置より抹消する。

【０００６】

【発明が解決しようとする課題】しかしながら、上記従来の第１の方法では、耐タンパ装置などの特別な装置を必要としていないが、データを転々流通させる際に問題が生じる。即ち、当該技術では、行使時の事後検出しか行えないため、流通過程では、当該データの有効性は判定できないという問題がある。

【０００７】従来の第２の方法では、耐タンパ装置を用いることにより、データの唯一性を保証することができる。また、（特願平６－５０３９１３）や、（特開平９－５１１３５０）などで述べられている方式などを併用し、暗号によって保護された安全な通信路を介して耐タンパ装置を結合し、当該通信路を介してデータの授受を行うことにより、当該データの流通を、複製を事前に防止しながら行うことを可能とする。しかしながら、当該技術は、耐タンパ装置の中にデータを格納する必要があるため、以下の２点が問題となる。

【０００８】まず、データの記述そのものを見ることができなくなるため、記述の正当性の検証など、複製に関する有効性以外の検証も全て当該耐タンパ装置に委ねなければならないという制約が生じる。

【０００９】また、データの格納部のみならず、データの取扱に必要な処理も全て耐タンパ装置が負わなければならないため、耐タンパ装置に対して記憶容量や処理速度に大きな要求が発生する。特に、現時点で耐タンパ装置として一般的なＩＣカードでは、処理速度や記憶容量に不足が生じる。

【００１０】本発明は、上記の点に鑑みなされたもので、データの有効な複製数を一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証をすべて耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させる原本データ流通方法、原本データ流通システム及び装置、並びに原本データ流通プログラムを記録した記録媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記の目的を達成させるために、本発明は、次のように構成される。

【００１２】本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、データを発行する発行者装置に対応する第１の情報を生成する手段と、該第１の情報を転送する手段と、データに対応する第２の情報を転送する手段とを有する装置と、受信した第１の情報の有効性を判定する手段と、有効な第１の情報に対応する発行者装置が正当なものであるかどうかを検証し、正当である場合に前記第２の情報に対応するデータを有効と判定する手段とを有する装置とを有する。

【００１３】ここでの第１の情報は、例えば、後述するH(PkＩ)である。また、第２の情報は、例えば、データやデータのハッシュ値である。発行者装置が正当なものであるかどうかは、例えば、上記第２の情報の転送元装置と第１の情報に対応する装置とが同一であるとき、も

しくは該転送元装置が耐タンパ装置であると認証されたときに有効であると判定する。これらの原本性情報の認証処理を耐タンパ装置等が行うことによって、データの取扱に必要な処理も全て耐タンパ装置等が負わなければならないという従来の問題点を解消することができ、処理速度や記憶容量等の処理負荷を低減させることが可能となる。

【００１４】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積方法であり、電子的な情報の発行者装置による該電子的な情報に対する署名である第３の情報を付与するステップと、前記発行者装置により前記第３の情報が付与された電子的な情報と対応する第４の情報を生成するステップと、電子的な情報利用装置において、前記第３の情報と前記第４の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するステップとを有する。

【００１５】ここで、第４の情報は、例えば、署名付きデータのハッシュ値として構成されるマニフェストである。マニフェストは原本性情報に対応するものである。これにより、本発明によれば、データ及び当該データに対応する署名を格納し、データと署名付きデータに１対１に対応する情報であるマニフェストを格納し、署名の生成者である署名者を特定し、マニフェストを格納しようとする者が署名者と同一であるかどうかを検証することにより、署名者の意図した数のマニフェストがデータ蓄積システム内に格納される。

【００１６】また、本発明は、第４の情報の格納と、署名者の同一性の判定とを、耐タンパ装置を用いて行う。

【００１７】これにより、耐タンパ装置を用いることで、データをデータ蓄積システム以外に格納することが可能となる。

【００１８】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、電子的な情報に第３の情報を付与し、該電子的な情報と対応するマニフェストの第４の情報を生成する発行者装置と、前記第３の情報と前記第４の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する利用者装置とを有する。

【００１９】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を利用する利用者装置であって、署名が付与された電子的な情報の格納及び抽出を行うための第１の格納手段と、前記電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、該マニフェストが正当であるかどうかを検証する第１の認証手段と、該マニフェストが正当であることが前記第１の認証手段により検証された時のみ、該マニフェストを前記第２の格納手段に格納する第１の制御手段とを有する。

【００２０】これにより、データに対応するマニフェストがデータ蓄積システムに格納されている時のみ、当該データが有効であると区別することにより、マニフェストの数を越えて有効なデータが存在することを防止する。

【００２１】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を発行する発行者装置であって、前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、該電子的な情報及び該信任情報に署名を付与する署名手段と、マニフェストを生成するマニフェスト生成手段と、該電子的な情報及び該信任情報を利用者装置に送信する手段と、該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信する手段と、該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信する手段とを有する。

【００２２】これにより、データの署名者が信用する署名者である信任対象を指定し、マニフェストに、発行者装置を署名者とする署名を付与し、マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び信任情報の署名者と、データの署名者とが同一であることを検証する。これにより、当該データの署名者が信用する経路のみを介してマニフェストを移送することが可能となる。さらに、このとき、耐タンパ装置を利用することにより、耐タンパ性が保証される。

【００２３】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報の権利を行使する対象である改札者装置であって、利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信する手段と、システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信する手段と、該利用者装置からマニフェストと該セッション情報を含む情報を受信する手段と、該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証する手段を有する。

【００２４】これにより、本発明では、システム内で一意性を持つセッション情報を生成し、セッション情報を格納することにより、暗号化された通信路を介することなく、１つのマニフェストが複数の格納部に格納されることを防止することが可能となると共に、複数のマニフェストを１つの格納部に並行に転送することが可能となる。

【００２５】上記の目的を達成するために、本発明は次のように構成することができる。なお、以下の発明は、後述する第２の実施例において詳細に説明される。

【００２６】本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける原

本データ流通方法であって、第１の装置が、ある装置に対応する第５の情報と、データもしくは、データに対応する情報である第６の情報と、から構成される原本性情報を転送する転送ステップと、第２の装置が前記原本性情報の転送元装置を検証し、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証ステップと、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該第２の装置が該原本性情報を有効であると判別する第２の認証ステップとを有する。

【００２７】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、ある装置に対応する第５の情報と、データもしくは、データに対応する情報である第６の情報と、から構成される原本性情報を転送する転送手段を有する第１の装置と、前記原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証手段と、該転送元装置と該原本性情報の第５の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証手段とを有する第２の装置とを有する。

【００２８】ここで、上記の第５の情報は、例えば、ある装置の検証鍵（公開鍵）のハッシュ値である。また、第６の情報は、例えば、データのハッシュ値である。第５の情報と第６の情報とからなる原本性情報はトークンと称される。上記の発明によれば、第２の認証手段が、転送元装置と前記第５の情報に対応する装置とが同一の場合に原本性情報が有効であると判別するため、データの取扱に必要な処理も全て耐タンパ装置等が負わなければならないという従来の問題点を解消することができ、処理速度や記憶容量等の処理負荷を低減させることが可能となる。また、署名を流通させる必要がないため、更に、処理速度や記憶容量等の処理負荷を低減させることが可能となる。

【００２９】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける発行者装置であって、自装置に対応する情報を第５の情報とし、あるデータもしくは、該データに対応する情報を第６の情報として、原本性情報を生成する原本性情報生成手段と、前記原本性情報を転送する原本性情報転送手段とを有する。

【００３０】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける利用者装置であって、ある装置に対応する第５の情報と、データもしくは、データに対応する情報である第６の情報から構成される原本性情報を転送する原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第５の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、前記認証手段で前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する。

【００３１】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける改札者装置であって、原本性情報の転送元装置を特定する特定手段と、前記転送元装置を認証する認証手段と、前記認証手段において、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第６の情報に対応するデータに対応する処理を行うデータ処理手段を有する。

【００３２】また、本発明においては、信用される第三者を特定するフィンガープリントを用いることによって、信用された特定の装置の間だけで原本性情報を流通させることとしている。

【００３３】また、本発明は、自装置に対応する情報を第５の情報とし、あるデータもしくは、該データに対応する情報を第６の情報として、原本性情報を生成する第１の原本性情報生成手段と、該原本性情報を転送する第１の原本性情報転送手段とを有する発行者装置と、ある装置に対応する第５の情報と、データもしくは、データに対応する情報である第６の情報から構成される原本性情報を転送する第２の原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第５の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証手段と、該第１の認証手段で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置と、原本性情報の転送元装置を特定する第２の特定手段と、前記転送元装置を認証する第２の認証手段と、該第２の認証手段において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第６の情報に対応するデータに対する処理を行うデータ処理手段を有する改札者装置とを有する。

【００３４】これにより、発行者装置、利用者装置及び改札者装置を有するシステムを構成することにより、これらの装置間において、チケット発行、チケットの譲渡、チケットの消費及びチケットの提示等の各処理を行うことが可能となる。

【００３５】

【発明の実施の形態】以下、図面と共に本発明の実施例を説明する。

（第１の実施例）まず、本発明の原本データ流通システムとしてのデータ蓄積システムについて説明する。

【００３６】図１は、本発明の原理を説明するための図

である。

【００３７】本発明におけるデータ蓄積システムでは、電子的な情報の発行者装置により該電子的な情報に署名した第１の情報を付与し（ステップ１）、発行者装置により電子的な情報と対応するマニフェストの第２の情報を生成して、第１の情報に付与し（ステップ２）、電子的な利用者装置において、第１の情報と第２の情報を用いて電子的な情報の発行者装置の同一性を判定し（ステップ３）、電子的な情報の複製を防止する。

【００３８】図２は、本発明のデータ蓄積システムの全体構成を示す。同図では、権利を表象する電子情報である電子チケットをデータとして発行者が利用者に発行し、チケットを発行された利用者が別の利用者間に譲渡し、チケット譲渡された利用者がチケットを消費する際に、改札者がチケットの有効性を検証する場合を示している。

【００３９】同図において、チケットの発行者は、発行者装置１を有し、チケットの発行先となる利用者は利用者装置２を有している。チケットの発行の際には、発行者装置１と利用者装置２の間は、接続装置４を介して通信手段が確立される。この通信手段は、発行の開始から終了までの間のみ確立されていればよい。

【００４０】また、チケット譲渡の際には、発行時と同様に利用者装置２間で接続装置４を介して通信手段を確立し、チケットを利用者装置２間で転送する。

【００４１】チケットの改札者は、改札者装置３を有している。チケット改札の際には、発行時と同様に、利用者装置２と改札者装置３との間で接続装置４を介して、通信手段を確立し、改札者装置３にチケットを転送する。

【００４２】このように、本発明にかかるデータ蓄積システムは、一時的な相互通信手段を提供する接続装置４により接続された、１乃至複数の発行者装置１と、１乃至複数の利用者装置２と、１乃至複数の改札者装置３とから構成されるシステムである。

【００４３】ここで、図３から図６を用いて、上記データ蓄積システムを構成する各装置について説明する。以下に、説明で用いる式の意味を示す。

【００４４】$x \| y$とは、xとyの連接である。

【００４５】Hとは、一方向のハッシュ関数であり、$y=H(x)$を満たすようなxをyから求めることが困難であるという性質を持つ。このようなハッシュ関数として、米ＲＳＡ社のＭＤ５などが知られている。

【００４６】S_{Pk}とは、検証関数V_{Pk}により検証可能な電子署名を生成する署名関数である。

【００４７】V_{Pk}は、検証関数であり、$V_{Pk}(x \| S_{Pk}(x))=1$, $V_{Pk}(x \| other)=0$ $(other \neq S_{Pk}(x))$という性質を持つ。即ち、ある情報xが署名関数S_{Pk}により署名されたものであるかどうかを検証できる性質を持つ。また、電子署名$S_{Pk}(x)$がxに対するS_{Pk}による正しい署名であるかどうかを検証できる性質を持つ。

【００４８】Pkは、検証鍵であり、検証器Vに検証鍵Pkを与えることにより、V_{Pk}を構成することが可能であるという性質を持つ。署名が付与された検証鍵$Pk2 \| S_{Pk1}(Pk2)$を特に、Pk1によるPk2の鍵証明書と呼ぶ。

【００４９】以上で述べたような性質を持つS_{Pk}、V_{Pk}を実現するような電子署名方式として、日本電信電話のＥＳＩＧＮなどが知られている。

【００５０】図３は、本発明の一実施例の発行者装置の構成を示す。

【００５１】同図に示す発行者装置１は、制御部１１、署名部１２、データ生成部１３、マニフェスト生成部１４、信任情報生成部１５から構成される。

【００５２】制御部１１は、検証鍵PkIを保持し、チケットの流通を安全に行うための制御を行う。ここで、PkIは後述する署名部１２が備える署名関数S_{PkI}に対応する検証鍵である。制御部１１による制御の詳細については後述する。

【００５３】署名部１２は、署名関数S_{PkI}を備える。署名関数S_{PkI}は、発行者装置１毎にそれぞれ異なり、署名部１２により秘匿される。

【００５４】データ生成部１３は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データmを生成する。本発明に係るデータ蓄積システムでは、データmの記述内容についてなんら制限を持つものではないため、データmとして切符やコンサートチケットなどの一般的なチケットによって扱われる権利を表象する電子情報の他、プログラム、音楽、画像データなどを扱うことが可能である。

【００５５】また、外部からデータm_0を与え、$m=H(m_0)$とするなど、他のデータへの関連として構成することや、他のデータへの関連を含む構成とすることも可能である。このようにすることによって、発行時における耐タンパ装置２８への転送データ量を削減することができる。

【００５６】マニフェスト生成部１４は、一方向のハッシュ関数Hを備え、署名付きデータ$m \| S_{PkI}(m)$のマニフェスト$c(m, PkI)=H(m \| S_{PkI}(m))$を生成する。

【００５７】信任情報生成部１５は、信任情報$t=(t_I, t_C)$を生成する。(t_I, t_C)は、それぞれ以下のように構成される。

【００５８】

$t_I=PkI$

$t_C=\{H(PkC_1), H(PkC_2), \cdots, H(PkC_n)\}$

ここで、PkIは、制御部１１が保持する検証鍵、PkC_iは発行者が「信用する」第三者（後述）による署名を検証するための検証鍵である。

【００５９】図４は、本発明の一実施例の利用者装置の構成を示す。同図に示す利用者装置２は、制御部２１、格納部２２と、制御部２３、認証部２４、署名部２５、

番号生成部２６、格納部２７から構成する耐タンパ装置２８を有する。各部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンパ装置２８として、ＩＣカードや、ネットワーク経由で構成され、第三者により厳重に管理されたサーバなどが利用可能である。

【００６０】制御部２１は、耐タンパ装置２８に封入された制御部２３と共に、チケットの流通を安全に行うための制御を行う。制御部２１による制御の詳細については後述する。

【００６１】格納部２２は、利用者が保持する署名付きデータの集合M_U及び発行者による署名付きの信任情報の集合T_Uを格納する。これらの集合は、制御部２１により更新可能である。

【００６２】制御部２３は、検証鍵PkU，PkC及び鍵証明書$Pk_U \| S_{PkC}(Pk_U)$を保持し、制御部２１と共に、チケットの流通を安全に行うための制御を行う。ここでPkUは署名部２５が備えるS_{PkU}に対応する検証鍵であり、S_{PkC}は、ＩＣカード製造者もしくは、耐タンパサーバ管理者など、耐タンパ装置２８の安全性を保証する第三者により秘匿される署名関数である。即ち、署名関数S_{PkU}を含む耐タンパ装置２８は、署名関数S_{PkC}を保有する第三者により耐タンパ性が保証されている。制御部２３による制御の詳細については後述する。また、PkCは、S_{PkC}の検証鍵である。

【００６３】格納部２２は、接続装置４を介して他の利用者装置２の格納部２２や改札者装置３の格納部３４などと共用することも可能である。この場合、データmおよび信任情報(t_1，t_2，t_3)は利用者装置や改札者装置間で共用されることとなるため、以降の実施例においてそれら情報の転送は不要となる。

【００６４】認証部２４は、検証器Vを備える。

【００６５】署名部２５は、署名関数S_{PkU}を備える。S_{PkU}は、利用者装置２毎にそれぞれ異なり、署名部２５により秘匿される。

【００６６】番号生成部２６は、次番号r_Uを保持し、番号の払出しを要求されると、現在の番号r_Uの値を返却すると共に、r_Uをインクリメントする。

【００６７】格納部２７は、マニフェストの集合$C_U=\{c_1,c_2,\cdots,c_n\}$及び番号の集合$R_U=\{r_1,r_2,\cdots,r_m\}$を格納する。これらの集合は、制御部２１により更新可能である。

【００６８】図５は、本発明の一実施例の改札者装置の構成を示す。

【００６９】同図に示す改札者装置３は、制御部３１、認証部３２、番号生成部３３、及び格納部３４から構成される。

【００７０】制御部３１は、検証鍵PkVを備え、チケットの流通を安全に行うための制御を行う。制御部３１による制御の詳細については後述する。

【００７１】認証部３２は、検証器Vを備える。

【００７２】番号生成部３３は、次番号r_Vを保持し、番号の払出しを要求されると、r_Vを返却すると共に、r_Vをインクリメントする。

【００７３】格納部３４は、番号の集合$R_V=\{r_1,r_2,\cdots,r_m\}$を格納する。これらの集合は、制御部３１により更新可能である。

【００７４】図６は、本発明の一実施例の接続装置４の構成を示す。

【００７５】同図に示す接続装置４は、通信部４１を有する。通信部４１は、発行者装置１、利用者装置２、改札者装置３間や利用者装置２相互間での一時的もしくは、永続的な通信手段を提供する。ここで、接続装置４としてＩＣカード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数のＰＣなどが利用可能である。

【００７６】上述したような構成を有する各装置を用いて、電子チケットの流通を安全に行う方式を以下において説明する。

【００７７】以下で述べる流通方式における基本的な考え方は、以下のようなものである。

【００７８】・チケット本体は、発行者による署名付きのデータ$m \| S_{PkI}(m)$で表現されるものとする。mには、発行者がチケットの所有者に与える権利の内容が記述されている、もしくは、権利の内容が記述されているデータへの関連を含むものとする。

【００７９】・チケット発行者の署名S_{PkI}により、チケットの改竄は防止できる。

【００８０】・チケット本体の複製は、特に禁止しない。

【００８１】・チケット本体から、そのチケットに対応するマニフェスト$c(m, Pk_I)$を生成できる。このマニフェストは、事実上チケット本体に１対１に対応する。

【００８２】・マニフェストは、発行者が信用できる耐タンパ装置２８内の格納部２７に格納されることにより、「有効」なものとなる。

【００８３】・発行者が信用できる耐タンパ装置とは、発行者が信用する者によって耐タンパ性が保証された装置である。発行者が信用する者は、信任情報t_Iにより規定される。

【００８４】・チケットを消費もしくは、譲渡するためには、有効なマニフェストが必要である。

【００８５】・有効なマニフェストは、対応するチケットの発行者のみが新規に作成可能である。

【００８６】・１つの有効なマニフェストから、複数の有効なマニフェストを作成することを禁止する。即ち、利用者が他者が署名したチケット本体のマニフェストを勝手に作成することを不可能にする。

【００８７】以下、（１）チケット発行の場合、（２）チケット譲渡の場合、（３）チケット消費の場合、のそ

れぞれの場合に分けてチケットの流通方式を説明する。なお、各装置を跨がるそれぞれの通信は、接続装置４中の通信部４１を介するものとする。

【００８８】（１） チケット発行の場合：以下は、発行者装置１から利用者装置２に対する接続装置４を介したチケット発行処理の流れである。

【００８９】図７は、本発明の一実施例のチケット発行処理のシーケンスチャートである。ステップ１０１）制御部１１は、以下の手順によりm及び$S_{PkI}(m)$を得て、署名付きデータであるところのチケット$m \| S_{PkI}(m)$の生成を行う。

【００９０】（ａ） データ生成部１３によりデータmを生成する。

【００９１】（ｂ） 署名部１２にmを与え、$S_{PkI}(m)$を生成する。

【００９２】ステップ１０２） 制御部１１は、マニフェスト生成部１４にチケット$m \| S_{PkI}(m)$を与え、マニフェスト$c(m,PkI)$を生成する。

【００９３】ステップ１０３） 制御部１１は、以下の手順により信任情報t及び署名関数$S_{PkI}(t)$を得て、署名付き信任情報$t \| S_{PkI}(t)$の生成を行う。

【００９４】（ａ） 信任情報生成部１５により、信任情報tを生成する。tの構成は、前述の通りである。

【００９５】（ｂ） 署名部１２に信任情報ｔを与え、署名$S_{PkI}(t)$を生成する。

【００９６】ステップ１０４） 制御部１１は、制御部２１にチケット$m \| S_{PkI}(m)$と署名付き信任情報$t \| S_{PkI}(t)$を転送する。

【００９７】ステップ１０１においてデータ生成部１３が生成したmが別のデータへの関連、例えば$m=H(m_0)$などとして構成されている、ないし関連を含む場合は、必要に応じて該関連するデータ(m_0など)もあわせて転送する。これは、以降で述べるチケット譲渡の場合、チケット消費の場合も同様である。

【００９８】ステップ１０５） 制御部２１は、チケット$m \| S_{PkI}(m)$を格納部２２のM_Uに、署名付き信任情報$t \| S_{PkI}(t)$を格納部２２の信任情報の集合T_Uにそれぞれ追加して格納する。

【００９９】mに関連するデータも転送されてきた場合は、関連を検証し、該検証に失敗した場合は以降の処理を中断し、その旨を通知する。これは、以降で述べるチケット譲渡の場合、チケット消費の場合も同様である。

【０１００】ステップ１０６） 制御部２１は、制御部２３にセッション情報(s_1,s_2)の生成を依頼する。

【０１０１】制御部２３は、以下の手順により、セッション情報(s_1,s_2)を生成し、制御部２１に転送する。

【０１０２】（ａ） 番号生成部２６により、番号r_Uの払い出しを受ける。

【０１０３】（ｂ） r_Uを格納部２７の番号集合R_Uに追加する。

【０１０４】（ｃ） $(s_1,s_2)=(H(PkU),r_U)$を生成する。ここで、PkUは、制御部２１が保持する検証鍵である。

【０１０５】ステップ１０７） 制御部２１は、制御部１１にセッション情報(s_1,s_2)を転送する。

【０１０６】ステップ１０８） 制御部１１は、署名部１２が備えるS_{PkI}と制御部１１が保持する検証鍵PkIを用い、マニフェスト発行形式$e_I=(e_1,e_2,e_3,e_4,e_5)$を得る。ここで、$e_I$の各要素は以下の値をとる。

【０１０７】

$e_1=c(m,PkI)$

$e_2=s_1$

$e_3=s_2$

$e_4=S_{PkI}(c(m,PkI) \| s_1 \| s_2)$

$e_5=PkI$

ステップ１０９） 制御部１１は、制御部２１にマニフェスト発行形式e_Iを転送する。

【０１０８】ステップ１１０） 制御部２１は、制御部２３にチケット本体$m \| S_{PkI}(m)$とマニフェスト発行形式e_Iを転送し、e_I内のマニフェストの格納を依頼する。

【０１０９】ステップ１１１） 制御部２３は、認証部２４を用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１を介して、制御部１１に処理の中断の通知を行う。

【０１１０】

$e_2=H(PkU)$ （１）

$e_3 \in R_U$ （２）

$V_{e5}(m \| S_{PkI}(m))=1$ （３）

$V_{e5}(e_1 \| e_2 \| e_3 \| e_4)=1$ （４）

$e_1=H(m \| S_{PkI}(m))$ （５）

上記の式（１）及び式（２）は、セッション情報の正当性の検証である。この検証により、他の利用者装置２宛のマニフェスト発行形式を格納すること、及びマニフェスト発行形式の再利用によってマニフェストを複製すること、などの不正を防止する。式（３）及び式（４）は、マニフェスト発行形式に対する署名の正当性の検証である。この検証により、チケットの発行者が署名したマニフェスト発行形式に含まれるマニフェスト以外を格納することを防止する。式（５）はマニフェストとチケット本体の対応の検証である。この検証により、別のチケット本体に対応するマニフェストなど、該チケット本体に対応しないマニフェストの格納を防止する。

【０１１１】ステップ１１２） 制御部２３は、格納部２７の番号集合R_Uから$e_3(=r_U)$を削除する。

【０１１２】ステップ１１３） 制御部２３は、格納部２７のマニフェストの集合C_Uに$e_1(=c(m,PkI))$を追加する。

【０１１３】ステップ１１４） 制御部２３は、制御部２１にe_1を転送し、処理の正常終了を通知する。

【０１１４】（２） チケット譲渡の場合：以下は、利

用者装置２ａから利用者装置２ｂに対する接続装置４を介したチケット譲渡処理の流れである。

【０１１５】図8、図9は、本発明の一実施例のチケット譲渡処理のシーケンスチャートである。

【０１１６】ステップ２０１）　制御部２１ａは、格納部２２ａが保持する署名付きデータの集合M_{Ua}から譲渡対象となるチケット$m \| Sp_{kI}(m)$を抽出する。

【０１１７】ステップ２０２）　制御部２１ａは、格納部２２ａが保持するT_{Ua}から$m \| Sp_{kI}(m)$の発行者による署名付き信任情報$t \| Sp_{kI}(t)$を抽出する。

【０１１８】ステップ２０３）　制御部２１ａは、制御部２１ｂに$m \| Sp_{kI}(m)$と$t \| Sp_{kI}(t)$を転送する。

【０１１９】ステップ２０４）　制御部２１ｂは、$m \| Sp_{kI}(m)$を格納部２２ｂの署名付きデータの集合M_{Ub}に、$t \| Sp_{kI}(t)$を格納部２２の信任情報の集合T_{Ub}に、それぞれ格納する。

【０１２０】ステップ２０５）　制御部２１ｂは、制御部２３ｂにセッション情報(s_1,s_2)の生成を依頼する。制御部２３ｂは、以下の手順により(s_1,s_2)を生成し、制御部２１ｂに転送する。

【０１２１】（ａ）　番号生成部２６ｂにより番号r_{Ub}の払出しを受ける。

【０１２２】（ｂ）　r_{Ub}を格納部２７ｂの番号集合R_{Ub}に追加する。

【０１２３】（ｃ）　$(s_1,s_2)=(H(PkUb),r_{Ub})$を生成する。ここで、PkUbは、制御部２１ｂが保持する検証鍵である。

【０１２４】ステップ２０６）　制御部２１ｂは、制御部２１ａに(s_1,s_2)を転送する。

【０１２５】ステップ２０７）　制御部２１ａは、制御部２３ａに(s_1,s_2)と譲渡対象チケットのハッシュ$H(m \| Sp_{kI}(m))$を転送する。

【０１２６】ステップ２０８）　制御部２３ａは、格納部２７ａに格納されたマニフェスト集合C_{Ua}について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１ａに処理の失敗を通知する。

【０１２７】

$$H(m \| Sp_{kI}(m)) \in C_{Ua} \quad (6)$$

上記の式（６）は、譲渡対象チケットに対応するマニフェスト$c_{(m,PkI)}=H(m \| Sp_{kI}(m))$が格納部２７ａに格納されていることの検証である。

【０１２８】ステップ２０９）　制御部２３ａは、署名部２５ａが備えるSp_{kUa}と制御部１１が保持する検証鍵PkUa，PkCa及び鍵証明書$PkUa \| Sp_{kCa}(PkUa)$を用い、マニフェスト転送形式$e_C=(e_1,e_2,e_3,e_4,e_5,e_6,e_7)$を得る。ここで、$e_C$の各要素は、以下の値となる。

【０１２９】

$e_1=c(m,PkI)$

$e_2=s_1$

$e_3=s_2$

$e_4=Sp_{kUa}(c(m,PkI) \| s_1 \| s_2)$

$e_5=PkUa$

$e_6=Sp_{kCa}(PkUa)$

$e_7=PkCa$

ステップ２１０）　制御部２３ａは、マニフェスト集合C_{Ua}から$c_{(m,PkI)}$を削除する。

【０１３０】ステップ２１１）　制御部２３ａは、制御部２１ａにe_Cを転送する。

【０１３１】ステップ２１２）　制御部２１ａは、制御部２１ｂにe_Cを転送する。制御部２１ｂは、転送されたe_C中のe_1について、$e_1=H(m \| Sp_{kI}(m))$が成立することを検証する。

【０１３２】ステップ２１３）　制御部２１ｂは、制御部２３ｂにe_C，$t \| Sp_{kI}(t)$，$m \| Sp_{kI}(m)$を転送し、e_C内のマニフェストの格納を依頼する。

【０１３３】ステップ２１４）　制御部２３ｂは、認証部２４ｂを用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１ｂに処理の中断を通知する。

【０１３４】

$$e_2=H(PkUb) \quad (7)$$

$$e_3 \in R_{Ub} \quad (8)$$

$$V_{e5}(e_1 \| e_2 \| e_3 \| e_4,e_5)=1 \quad (9)$$

$$V_{e7}(e_5 \| e_6)=1 \quad (10)$$

$$H(e7) \in t_C \quad (11)$$

$$V_{tI}(m \| Sp_{kI}(m))=1 \quad (12)$$

$$V_{tI}(t \| Sp_{kI}(t))=1 \quad (13)$$

上記の式（７）及び式（８）は、セッション情報の正当性の検証である。この検証により、他の利用者装置２宛のマニフェスト転送形式を格納すること、及びマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

【０１３５】式（９）は、マニフェスト転送形式の署名者を特定するための検証であり、式（１０）は、該署名者の鍵証明書の検証であり、式（１１）は、当該鍵証明書の署名者が、信任情報中の信任対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

【０１３６】式（１２）及び式（１３）は、当該信任情報に対する署名の正当性の検証である。この検証により、当該信任情報が当該チケットの署名者により正しく署名されていることを確認する。

【０１３７】ステップ２１５）　制御部２３ｂは、格納部２７ｂの番号の集合R_{Ub}から$e_3(=r_{Ub})$を削除する。

【０１３８】ステップ２１６）　制御部２３ｂは、格納部２７ｂのマニフェスト集合C_{Ub}にe_1（$=c_{(m,PkI)}$）を追加する。

【０１３９】ステップ２１７）　制御部２３ｂは、制御部２１ｂに処理の正常終了を通知する。

【０１４０】ステップ２１８）　制御部２１ｂは、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は、処理の正常終了を、制御部２１ａに通知する。

（３）　チケット消費の場合：以下は、利用者装置２から改札者装置３に対する、接続装置４を介したチケット消費処理の流れである。

【０１４１】図１０は、本発明の一実施例のチケット消費のシーケンスチャートである。

【０１４２】ステップ３０１）　制御部２１は、格納部２２が保持する署名付きデータの集合M_Uから消費対象となるチケット$m \| S_{PkI}(m)$を抽出する。

【０１４３】ステップ３０２）　制御部２１は、格納部２２が保持する署名付き信任情報の集合T_Uから$m \| S_{PkI}(m)$の発行者による署名付き信任情報$t \| S_{PkI}(t)$を抽出する。

【０１４４】ステップ３０３）　制御部２１は、制御部３１に$m \| S_{PkI}(m)$と$t \| S_{PkI}(t)$を転送する。

【０１４５】ステップ３０４）　制御部３１は、以下の手順によりセッション情報(s_1,s_2)を生成する。

【０１４６】（ａ）　番号生成部３３により番号r_Vの払出しを受ける。

【０１４７】（ｂ）　r_Vを格納部３４の番号集合R_Vに追加する。

【０１４８】（ｃ）　$(s_1,s_2)=(H(Pk_V),r_V)$を生成する。Pk_Vは制御部３１が保持する検証鍵である。

【０１４９】ステップ３０５）　制御部３１は、制御部２１にセッション情報(s_1,s_2)を転送する。

【０１５０】ステップ３０６）　制御部２１は、制御部２３に、(s_1,s_2)と消費対象チケットのハッシュ$H(m \| S_{PkI}(m))$を転送する。

【０１５１】ステップ３０７）　制御部２３は、格納部２７に格納されたマニフェスト集合C_Uについて、以下の式が成立することを検証する。検証に失敗した場合には、以後の処理を中断し、制御部２１に処理の失敗を通知する。

【０１５２】

$$H(m \| S_{PkI}(m)) \in C_U \qquad (15)$$

上記の式（１５）は、消費対象チケットに対応するマニフェスト$c_{(m,PkI)}=H(m \| S_{PkI}(m))$が格納部２７に格納されていることの検証である。

【０１５３】ステップ３０８）　制御部２３は、署名部２５が備える署名関数S_{PkU}と制御部２１が保持する検証鍵PkU，PkC及び鍵証明書$Pk_U \| S_{PkC}(Pk_U)$を用い、マニフェスト転送形式$e_C=(e_1,e_2,e_3,e_4,e_5,e_6,e_7)$を得る。ここで、$e_C$の各要素は以下の値をとる。

【０１５４】

$e_1=c_{(m,PkI)}$

$e_2=s_1$

$e_3=s_2$

$e_4=S_{PkU}(c_{(m,PkI)} \| s_1 \| s_2)$

$e_5=Pk_U$

$e_6=S_{PkC}(Pk_U)$

$e_7=Pk_C$

ステップ３０９）　制御部２３は、マニフェスト集合C_Uから$c_{(m,PkI)}$を削除する。

【０１５５】ステップ３１０）　制御部２３は、制御部２１にe_Cを転送する。

【０１５６】ステップ３１１）　制御部２１は、制御部３１にe_Cを転送する。

【０１５７】ステップ３１２）　制御部３１は、認証部３２を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１に処理の中断を通知する。

【０１５８】

$$e_2=H(Pk_V) \qquad (16)$$

$$e_3 \in R_V \qquad (17)$$

$$V_{e5}(e_1 \| e_2 \| e_3 \| e_4,e_5)=1 \qquad (18)$$

$$V_{e7}(e_5 \| e_6)=1 \qquad (19)$$

$$H(e_7) \in t_C \qquad (20)$$

$$V_{tI}(m \| S_{PkI}(m))=1 \qquad (21)$$

$$V_{tI}(t \| S_{PkI}(t))=1 \qquad (22)$$

上記の式（１６）及び式（１７）は、セッション情報の正当性の検証である。この検証により、他の改札者装置３宛のマニフェスト転送形式を格納すること、及び自分宛のマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

【０１５９】式（１８）は、マニフェスト転送形式の署名者を特定するための検証であり、式（１９）は、当該署名者の鍵証明書の検証であり、式（２０）は、当該鍵証明書の署名者が信任情報中の信任対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

【０１６０】式（２１）及び式（２２）は、当該信任情報に対する署名の正当性の検証である。この検証により、当該信任情報が当該チケットの署名者により正しく署名されていることを確認する。

【０１６１】ステップ３１３）　制御部３１は、格納部３４のR_Vからe_3（$=r_V$）を削除する。

【０１６２】ステップ３１４）　制御部３１は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を制御部２１に通知する。検証に成功した場合は、mに対応するサービスを消費者に提供する。

【０１６３】

$$e_1=H(m \| S_{PkI}(m)) \qquad (23)$$

上記の式（２３）は、消費されたチケットに対応するマニフェストが転送されたことの検証である。この検証に

より、有効なマニフェストが併せて転送されたこと、即ち、有効なチケットが消費されたことを確認する。

【０１６４】また、前述の図2に示す発行者装置１、利用者装置２、改札装置３の各構成要素をプログラムとして構築し、発行者装置、利用者装置、改札装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスクやＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際に、各コンピュータにインストールすることにより容易に本発明を実現できる。

【０１６５】上述のように、本発明の第１の実施例によれば、データの署名者の意図した数だけマニフェストをデータ蓄積システムのマニフェスト格納部に格納し、当該署名者以外が該マニフェストを新たに格納することを防止する、該マニフェストの数を越えて有効なデータが存在することを防止する、当該署名者が信用する経路のみを介してマニフェストを移送することが可能となる。

【０１６６】チケットを本発明のデータ蓄積システムのデータとして用いることにより、チケット自体を耐タンパ装置に格納することなしに、チケットの有効な複製数を一定に保つことが可能となる。

【０１６７】また、プログラムを本発明におけるデータとして用い、当該プログラムの実行ライセンスをマニフェストとして用いることにより、不当に複製された当該プログラムの実行を防止することが可能となる。

【０１６８】また、音楽データや画像データを本発明におけるデータとして用い、当該データの鑑賞権をマニフェストとして用いることにより、不当に複製された当該データの鑑賞を防止することが可能となる。

【０１６９】さらに、データを鑑賞する毎に当該データを「消費（実施例における（３））」することにより、利用毎の課金システム（pay per view　課金）などに利用することが可能である。

【０１７０】（第２の実施例）以下、本発明の第２の実施例について説明する。

【０１７１】さて、上記の第１の実施例は、原本性を示すデータのみを耐タンパ装置に格納することにより、データの有効な複製数を常に一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証を全て耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させることを特徴としている。この発明は、従来の技術と比較すれば、顕著な効果を奏するが、実用上主に、以下の２点が問題といえる。

【０１７２】まず、原本性を示すデータの生成時に、データと該データに付与された署名を検証するためにデータ及び該データの署名を耐タンパ装置に転送しなくてはならず、その一方で、ＩＣカードの転送速度は、９６００bit/s程度（ＩＳＯ－７８１６）と比較的低速であるため、耐タンパ装置としてＩＣカードを用いると、該データの大きさによっては原本性を示すデータの生成に要する時間を著しく増大させる。

【０１７３】また、当該技術では、データに対して署名を付与したものに対して原本性を示すデータを生成し、消費の際にも該データ及び該署名を用いて原本性を示すデータの検証が必要となるため、該データのみならず、該署名も共に流通させる必要が生じ、これは、システムに構築のために必要な記憶容量や流通の際の処理時間を増大させる。

【０１７４】第２の実施例では、原本性を示すデータ（トークン）の生成やデータの流通などにおける負荷を低減する原本データ流通システムについて説明する。

【０１７５】図１１は、本発明の第２の実施例の原理構成図である。

【０１７６】第２の実施例における、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムは、自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成手段５１と、該原本性情報を転送する第１の原本性情報転送手段５２とを有する発行者装置５０と、ある装置に対応する第５の情報と、データもしくは、データに対応する情報である第６の情報から構成される原本性情報を転送する第２の原本性情報転送手段６１と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定手段６２と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証手段６３と、該第１の認証手段６３で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段６４とを有する利用者装置６０と、原本性情報の転送元装置を特定する第２の特定手段７１と、転送元装置を認証する第２の認証手段７２と、該第２の認証手段７２において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理手段７３を有する改札者装置７０とを有する。

【０１７７】図１２は、本発明の原本データ流通システムにおけるデータ蓄積システムの構成を示す。

【０１７８】同図において、チケットの発行者は、発行者装置１００を有し、チケットの発行先となる利用者は利用者装置２００を有している。チケットの発行の際には、発行者装置１００と利用者装置２００の間は、接続装置４００を介して通信手段が確立され、発行者装置１００で有効化されたチケットを利用者装置２００に転送する。

【０１７９】上記のこれらの装置は、図１２（ａ），（ｂ）などの構成をとることができる。同図（ａ）は、

利用者装置２００としてＩＣカードを用い、接続装置４００としてＩＣカードリーダライタを用いる際の代表的な構成を示し、同図（ｂ）は、利用者装置としてＩＣカードなどの耐タンパ装置を装備可能もしくは、安全な場所に保管されたＰＣを用い、接続装置４００としてネットワークを用いる際の代表的な構成を示す。なお、同図（ａ），（ｂ）の構成を混在させて用いることも可能である。

【０１８０】上記の通信手段は、チケットの発行の開始から終了までの間のみ確立させていればよい。以下、「譲渡」、「消費」、「提示」の際にもこれは同様である。

【０１８１】チケット譲渡の際には、発行時と同様に利用者装置２００間で接続装置４００を介して通信手段を確立し、有効なチケットを利用者装置２００間で転送する。

【０１８２】チケットの改札者は、改札者装置３００を有している。チケット消費の際には、発行時と同様に利用者装置２００と改札者装置３００との間で接続装置４００を介して通信手段を確立し、利用者装置２００から改札者装置３００に有効なチケットを転送する。

【０１８３】チケット提示の際には、２つの利用者装置２００の間、もしくは利用者装置２００と改札者装置３００との間で、接続装置４００を介して通信手段を確立し、利用者装置２００から他の利用者装置２００もしくは、改札者装置３００に有効なチケットを所持していることの証明を転送する。

【０１８４】このように、本発明に係るデータ蓄積システムは、一時的な相互通信手段を提供する１つまたは、複数の接続装置４００により接続された、１つまたは、複数の発行者装置１００と、１つまたは、複数の利用者装置２００と、１つまたは、複数の改札者装置３００とから構成されるシステムである。

【０１８５】以下、図面と共に本発明の実施例を説明する。

【０１８６】図１３から図１６を用いて、上記のデータ蓄積システムを構成する各装置について説明する。最初に、以下の説明で用いる式の意味については、ほぼ第１の実施例におけるものと同等である。

【０１８７】ここでは、検証鍵Pk2及びS_{PkI}によるPk2の電子署名S_{PkI}(Pk2)の組(Pk2,S_{PkI}(Pk2))を特に、PkIによるPk2の鍵証明書と呼ぶ。また、H(Pk)を特に、Pkのフィンガープリントと呼ぶ。

【０１８８】図１３は、本発明の一実施例の発行者装置の構成を示す。

【０１８９】図１３に示す発行者装置１００は、制御部１１０、署名部１２０、データ生成部１３０、トークン生成部１４０、信任情報生成部１５０から構成される。

【０１９０】制御部１１０は、検証鍵PkIを保持し、チケットの流通を安全に行うための制御を行う。ここで、PkIは、後述する署名部１２０が備える署名関数S_{PkI}に対応する検証鍵であり、そのフィンガープリントH(PkI)は、発行者を特定する識別子として用いられる。制御部１１０による制御の詳細については、後述する。

【０１９１】署名部１２０は、署名関数S_{PkI}を備える。S_{PkI}は、発行者装置１００毎にそれぞれ異なり、署名部１２０により秘匿される。

【０１９２】データ生成部１３０は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データmを生成する。本発明に係るデータ蓄積装置では、データmの記述内容についてなんら制限を持つものではないため、データmとして切符やコンサートチケットなどの一般的チケットによって扱われる権利を表象する電子情報のほか、プログラム、音楽、画像データなどを扱うことが可能である。

【０１９３】トークン生成部１４０は、一方向ハッシュ関数Hを備え、データm及び検証鍵PkIよりトークン

$(c_1,c_2)=(H(m),H(PkI))$

を生成する。ここで、c_2は、トークン発行者情報であり、当該トークンの発行者と発行者装置を特定するフィンガープリントである。ここでは、c_1にデータmのハッシュ値を用いたが、これにはmを識別する識別子などを用いることも可能である。

【０１９４】信任情報生成部１５０は、信任情報(t_1, t_2,t_3)を生成する。(t_1,t_2,t_3)は、署名部１２を用いて例えば、以下のように構成される。

【０１９５】

$t_1=\{H(PkA_1),H(PkA_2),\cdots,H(PkA_n)\}$

$t_2=S_{PkI}(H(PkA_1)\|H(PkA_2)\|\cdots\|H(PkA_n))$

$t_3=PkI$

ここで、$H(PkA_i)$は、発行者が「信用する」第三者（後述）を特定するフィンガープリントである。

【０１９６】ここで、信任情報は以下で示す(t'$_1$, t'$_2$,t'$_3$,t'$_4$)のように構成することも可能である。

【０１９７】

t'$_1=\{H(PkA_1),H(PkA_2),\cdots,H(PkA_n)\}$

t'$_2=H(m)$

t'$_3=S_{PkI}(H(PkA_1)\|H(PkA_2)\|\cdots\|H(PkA_n)\|H(m))$

t'$_4=PkI$

この場合、$H(PkA_i)$は、発行者が「データmを流通させるにあたって信用するに足りる」第三者を特定するフィンガープリントである。

【０１９８】また、上記信任情報は、第三者がさらに信任情報を発行することにより再帰的に構築することも可能である。

【０１９９】また、さらに、信任情報を各発行者が生成することをせず、後述する利用者装置の耐タンパ装置の制御部や、改札者装置の制御部が予め固定的に保持しておく形態を採ることも可能である。この場合、署名は必要なく、以下で示す(t"$_1$,t"$_2$)もしくは、t"$_1$のみと

して信任情報を構成できる。

【０２００】

$t''_1=\{H(PkA_1),H(PkA_2),\cdots,H(PkA_n)\}$

$t''_2=H(m)$

この場合、$H(PkA_1)$は、当該制御部（を作成した第三者）が、「（データmを流通させるにあたって）信用する」第三者を特定するフィンガープリントである。

【０２０１】以下においては、信任情報は(t_1,t_2,t_3)と構成されるものとして説明するが、上記のいずれの信任情報を用いる場合も容易に類推可能である。

【０２０２】図１４は、本発明の一実施例の利用者装置の構成を示す。

【０２０３】同図に示す利用者装置２００は、制御部２１０、格納部２２０と、制御部２３０、認証部２４０、署名部２５０、番号生成部２６０、格納部２７０から構成される耐タンパ装置２８０を有する。耐タンパ装置２８０は、各構成部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンパ装置２８０として、ＩＣカードや、ネットワーク経由で接続され、第三者により厳重に管理されたサーバなどが利用可能である。

【０２０４】制御部２１０は、発行者情報

$I_U=\{H(PkI_1),H(PkI_2),\cdots,H(PkI_n)\}$

を備え、耐タンパ装置２８０に封入された制御部２３と共に、チケットの流通を安全に行うための制御を行う。ここで、I_Uは、利用者から「信用された」発行者を示す集合であり、当該利用者により任意の時点で更新可能である。制御部２１０は、I_Uに含まれる発行者により発行されたトークンのみを有効であると判断する。制御部２１０による制御の詳細については、後述する。

【０２０５】また、I_Uをデータごとに発行者情報の集合を管理すること、すなわち$I_U(m_i)=\{H(PkI_{i1}),H(PkI_{i2}),\cdots,H(PkI_{in})\}$として実現することも可能である。

【０２０６】格納部２２０は、利用者が保持するデータの集合M_U及び信任情報の集合T_Uを格納する。これらの集合は、制御部２１０により更新可能である。

【０２０７】制御部２３０は、検証鍵PkU,PkA及び鍵証明書$(PkU,S_{PkA}(PkU))$を保持し、制御部２１０と共に、チケットの流通を安全に行うための制御を行う。ここで、PkUは、署名部２５０が備えるS_{PkU}に対応する検証鍵であり、そのフィンガープリントH(PkU)は、該利用者装置を特定する識別子として用いる。S_{PkA}は、ＩＣカード製造者もしくは耐タンパサーバの管理者など、耐タンパ装置２８０の安全性を保証する第三者により秘匿される署名関数である。すなわちS_{PkU}を含む耐タンパ装置２８０は、S_{PkA}を保持する第三者により耐タンパ性を保証されている。制御部２３０による制御の詳細については後述する。また、PkAは、S_{PkA}の検証鍵である。

【０２０８】認証部２４０は、検証器Vを備える。

【０２０９】署名部２５０は、署名関数S_{PkU}を備える。S_{PkU}は、利用者装置２００毎にそれぞれ異なり、署名部２５０により秘匿される。

【０２１０】番号生成部２６０は、次番号r_Uを保持し、番号の払出しを要求されると当該時点のr_Uの値を返却すると共にr_Uをインクリメントする。ここで、r_Uは正数である。

【０２１１】格納部２７０は、トークンの集合C_U及び番号の集合R_Uを格納する。これらの集合は、制御部２３０により更新可能である。

【０２１２】図１５は、本発明の一実施例の改札者装置の構成を示す。

【０２１３】制御部３１０は、検証鍵PkE及び、発行者情報

$I_E=\{H(PkI_1),H(PkI_2),\cdots,H(PkI_n)\}$

を備え、チケットの流通を安全に行うための制御を行う。ここで、I_Eは、改札者から「信用された」発行者を示す集合であり、当該改札者により任意の時点で更新可能である。制御部３１０は、I_Eに含まれる発行者により発行されたトークンのみを正当と判断し、当該トークンを伴うチケットの消費に対してのみサービスを提供する。制御部３１０による制御の詳細については後述する。

【０２１４】また、制御部２１０におけるI_Uと同様に、I_E をデータごとに発行者情報の集合を管理する、すなわち$I_E(m_i)=\{H(PkI_{i1}),H(PkI_{i2}),\cdots,H(PkI_{in})\}$として実現することも可能である。

【０２１５】認証部３２０は、検証器Vを備える。

【０２１６】番号生成部３３０は、次番号r_Eを保持し、番号の払出しを要求されると該時点のr_Eを返却すると共に、r_Eをインクリメントする。ここで、r_Eは正数である。

【０２１７】格納部３４０は、番号の集合R_Eを格納する。これらの集合は、制御部３１０により更新可能である。

【０２１８】図１６は、本発明の一実施例の接続装置の構成を示す。

【０２１９】同図によれば、接続装置４００は、通信部４１０から構成される。

【０２２０】通信部４１０は、発行者装置１００、利用者装置２００、改札者装置３００間や、利用者装置２００相互間での、一時的もしくは永続的な通信手段を提供する。ここで、接続装置４００として、ＩＣカード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数のＰＣ（パーソナルコンピュータ）などが利用可能である。

【０２２１】上述したような構成を有する各装置１００～４００を用いて電子チケットの流通を安全に行う方式を以下（１）チケットの発行の場合、（２）チケットの譲渡の場合、（３）チケットの消費の場合、のそれぞれの場合に分けて説明する。なお、各装置を跨がるそれぞ

れの通信は、接続装置４００中の通信部４１０を介するものとする。

【０２２２】（１）　チケット発行の場合：図１７は、本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャートである。なお、同図では、発行者装置１００と利用者装置２００との間に存在する接続装置４００は省略してある。

【０２２３】ステップ１１０１）　発行者装置１００の制御部１１０は、データ生成部１３０により、データmを生成する。当該データmを権利情報が記述されたチケットであるとする。

【０２２４】ステップ１１０２）　発行者装置１００の制御部１１０は、トークン生成部１４０にmおよびPkIを与え、トークン$(c_1,c_2)=(H(m),H(PkI))$を生成する。

【０２２５】ステップ１１０３）　制御部１１０は、信任情報生成部１５０により、信任情報(t_1,t_2,t_3)を生成する。信任情報の構成は前述の通りである。

【０２２６】ステップ１１０４）　制御部１１０は、利用者装置２００の制御部２１０にmと(t_1,t_2,t_3)を転送する。

【０２２７】ステップ１１０５）　利用者装置２００の制御部２１０は、mを格納部２２０のM_Uに、(t_1, t_2, t_3)を格納部２２０のT_Uに、それぞれ追加して格納する。

【０２２８】ステップ１１０６）　制御部２１０は、耐タンパ装置２８０の制御部２３０にセッション情報(s_1, s_2)の生成を依頼し、制御部２３０は、以下の手順により(s_1,s_2)を生成し、制御部２１０に転送する。

【０２２９】（ａ）　耐タンパ装置２８０の番号生成部２６０により番号r_Uの払出しを受ける。

【０２３０】（ｂ）　r_Uを格納部２７０の番号集合R_Uに追加する。

【０２３１】（ｃ）　$(s_1,s_2)=(H(PkU),r_U)$を生成する。ここで、PkUは、制御部２１０が保持する検証鍵である。

【０２３２】ステップ１１０７）　制御部２１０は、発行者装置１００の制御部１１０に(s_1,s_2)を転送する。

【０２３３】ステップ１１０８）　発行者装置１００の制御部１１０は、署名部１２０が備えるS_{PkI}と制御部１１０が保持する検証鍵PkIを用い、トークン交換形式$e=(e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8)$を得る。ここで、eの各要素は、以下の値となる。また、チケット発行の際においてはe_7及びe_8はダミーであり、それぞれ任意の値を持たせてよい。

【０２３４】

$e_1=c_1$

$e_2=c_2$

$e_3=s_1$

$e_4=s_2$

$e_5=S_{PkI}(c_1 \| c_2 \| c_3 \| c_4)$

$e_6=PkI$

$e_7=$ａｎｙ（任意）

$e_8=$ａｎｙ（任意）

ステップ１１０９）　発行者装置１００の制御部１１０は、利用者装置２００の制御部２１０にeを転送する。

【０２３５】ステップ１１１０）　利用者装置２００の制御部２１０は、耐タンパ装置２８０の制御部２３０にeを転送し、e内のトークンの格納を依頼する。

【０２３６】ステップ１１１１）　耐タンパ装置２８０の制御部２３０は、認証部２４０を用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１０を介して、発行者装置１００の制御部１１０に処理を中断を通知する。

【０２３７】

$e_3=H(PkU)$　（１）

$e_4 \in R_U$　（２）

$V_{e6}(e_1 \| e_2 \| e_3 \| e_4,e_5)=1$　（３）

$e_2=H(e_6)$　（４）

上記の式（１）及び式（２）は、セッション情報の正当性の検証である。この検証により、当該利用者装置２以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【０２３８】式（３）は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

【０２３９】また、式（４）は、トークン発行者情報の正当性の検証であり、当該トークンの署名者以外が発行者となるトークンを格納することを防止する。

【０２４０】ステップ１１１２）　利用者装置２００の耐タンパ装置２８０の制御部２３０は、格納部２７０のR_Uから$e_4(=r_U)$を削除する。

【０２４１】ステップ１１１３）　耐タンパ装置２８０の制御部２３０は、格納部２７０のC_Uに(e_1,e_2)を追加する。

【０２４２】ステップ１１１４）　耐タンパ装置２８０の制御部２３０は、制御部２１０に(e_1,e_2)を転送し、処理の正常終了を通知する。

【０２４３】ステップ１１１５）　制御部２１０は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は処理の正常終了を、発行者装置１００の制御部１１０に通知する。

【０２４４】

$e_1=H(m)$　（５）

$e_2 \in I_U$　（６）

式（５）及び式（６）は、転送されたトークンが、対象とするチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、発行されたチケットが有効であることを確認する。

【０２４５】（２）　チケット譲渡の場合：以下は、利

用者装置２００ａから利用者装置２００ｂに対する、接続装置４００を介したチケット譲渡処理の流れである。

【０２４６】図１８、図１９は、本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャートである。なお、同図において２つの利用者装置２００ａ，２００ｂの間に存在する接続装置４００は省略してある。また、利用者装置２００ａの各構成要素の各々にはａを付し、利用者装置２００ｂの各構成要素の各々にはｂを付す。

【０２４７】ステップ２２０１）　利用者装置２００ａの制御部２１０ａは、格納部２２０ａが保持するM_{Ua}から譲渡対象となるチケットｍを抽出する。

【０２４８】ステップ２２０２）　利用者装置２００ａの制御部２１０ａは、格納部２２０ａが保持するT_{Ua}からｍの発行者による信任情報(t_1,t_2,t_3)を抽出する。

【０２４９】ステップ２２０３）　制御部２１０ａは、利用者装置２００ｂの制御部２１０ｂにｍと(t_1,t_2,t_3)を転送する。

【０２５０】ステップ２２０４）　利用者装置２００ｂの制御部２１０ｂは、ｍを格納部２２０ｂのM_{Ub}に、(t_1,t_2,t_3)を格納部２２０ｂのT_{Ub}にそれぞれ格納する。

【０２５１】ステップ２２０５）　制御部２１０ｂは、耐タンパ装置２８０ｂの制御部２３０ｂにセッション情報(s_1,s_2)の生成を依頼する。制御部２３０ｂは、以下の手順により(s_1,s_2)を生成し、制御部２１０ｂに転送する。

【０２５２】（ａ）　耐タンパ装置２８０ｂの番号生成部２６０ｂにより番号r_{Ub}の払出しを受ける。

【０２５３】（ｂ）　r_{Ub}を耐タンパ装置２８０ｂの格納部２７０ｂの番号集合R_{Ub}に追加する。

【０２５４】（ｃ）　$(s_1,s_2)=(H(PkUb),r_{Ub})$を生成する。ここで、PkUbは、制御部２１０ｂが保持する検証鍵である。

【０２５５】ステップ２２０６）　制御部２１０ｂは、利用者装置２００の制御部２１０ａに(s_1,s_2)を転送する。また、I_{Ub}をあわせて転送するようにしてもよい。発行者情報の事前通知を行うことによって、式（１６）や式（２６）の検証に失敗するようなトークン交換形式を生成、送信することを未然に防止できる。

【０２５６】ステップ２２０７）　利用者装置２００ａの制御部２１０ａは、耐タンパ装置２８０ａの制御部２３０ａに(s_1,s_2)と譲渡対象チケットのハッシュH(m)を転送する。

【０２５７】ステップ２２０８）　利用者装置２００ａの耐タンパ装置２８０ａの制御部２３０ａは、格納部２７０ａに格納されたC_{Ua}について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１０ａに処理の失敗を通知する。

【０２５８】

$$\exists c_2((H(m),c_2)\in C_{Ua}),\quad c_2\in I_{Ub} \qquad (7)$$

式（７）は、譲渡対象チケットｍに対応するトークン$(H(m),c_2)$が耐タンパ装置２８０の格納部２７０ａに格納されていることの検証である。

【０２５９】ステップ２２０９）　耐タンパ装置２８０ａの制御部２３０ａは、署名部２５０ａが備えるS_{PkUa}と利用者装置２００ａの制御部２１０ａが保持する検証鍵PkUa，PkAa及び、鍵証明書$(PkUa,S_{PkAa}(PkUa))$を用い、トークン交換形式$e=(e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8)$を得る。ここで、eの各要素は以下の値をとる。

【０２６０】

$e_1=H(m)$

$e_2=c_2$

$e_3=s_1$

$e_4=s_2$

$e_5=S_{PkUa}(H(m)\|c_2\|s_1\|s_2)$

$e_6=PkUa$

$e_7=S_{PkAa}(PkUa)$

$e_8=PkAa$

ステップ２２１０）　利用者装置２００ａの耐タンパ装置２８０ａの制御装置２３０ａは、s_2が正であるなら、C_{Ua}から$(H(m),c_2)$を削除する。

【０２６１】ステップ２２１１）　耐タンパ装置２８０ａの制御部２３０ａは、制御部２１０ａにｅを転送する。

【０２６２】ステップ２２１２）　制御部２１０ａは、利用者装置２００ｂの制御部２１０ｂにｅを転送する。

【０２６３】ステップ２２１３）　制御部２１０ｂは、耐タンパ装置２８０ｂの制御部２３０ｂにｅと対応する信任情報ｔを転送し、e内のトークンの格納を依頼する。

【０２６４】ステップ２２１４）　制御部２３０ｂは、認証部２４０ｂを用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１０ｂに処理の中断を通知する。

【０２６５】

$$e_3=H(PkUb) \qquad (8)$$

$$e_4\in R_{Ub} \qquad (9)$$

$$V_{e6}(e_1\|e_2\|e_3\|e_4,e_5)=1 \qquad (10)$$

$$V_{e8}(e_6,e_7)=1 \qquad (11)$$

$$H(e_8)\in t_1 \qquad (12)$$

$$V_{t3}(t_1,t_2)=1 \qquad (13)$$

$$e_2=H(t_3) \qquad (14)$$

式（８）及び式（９）は、セッション情報の正当性の検証である。この検証により、当該利用者装置２００ｂ以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【０２６６】式（１０）は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

【０２６７】式（１１）は、当該署名者の鍵証明書の検証である。また、式（１２）は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式（１３）は、該信任情報の正当性の検証であり、式（１４）は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンパ性が保証されていることを確認する。

【０２６８】ステップ２２１５）　利用者装置２００の耐タンパ装置２８０ｂの制御部２３０ｂは、格納部２７０ｂのR_{Ub}から$e_4(=r_{Ub})$を削除する。

【０２６９】ステップ２２１６）　制御部２３０ｂは、格納部２７０ｂのC_{Ub}に(e_1,e_2)を追加する。

【０２７０】ステップ２２１７）　制御部２３０ｂは、制御部２１０ｂに処理の正常終了を通知する。

【０２７１】ステップ２２１８）　制御部２１０ｂは、以下の式が成立することを検証する。検証に失敗した場合は処理の中断を、検証に成功した場合は処理の正常終了を、制御部２１０ａに通知する。

【０２７２】

$$e_1=H(m) \qquad (15)$$

$$e_2 \in I_{Ub} \qquad (16)$$

式（１５）及び式（１６）は、転送されたトークンが、対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、譲渡されたチケットが有効であることを確認する。

【０２７３】制御部２１０ｂにおいて発行者情報がデータごとに管理されている場合は、式（１６）は$e_2 \in I_{Ub}(m)$となる。

【０２７４】（３）　チケット消費の場合：以下は、利用者装置２００から改札者装置３００に対する接続装置４００を介したチケット消費処理の流れである。

【０２７５】図２０は、本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャートである。

【０２７６】なお、同図において、利用者装置２００と改札者装置３００間に存在する接続装置４００は省略する。

【０２７７】ステップ３３０１）　利用者装置２００の制御部２１０は、格納部２２０が保持するM_Uから譲渡対象となるチケットｍを抽出する。

【０２７８】ステップ３３０２）　制御部２１０は、格納部２２０が保持するT_U からｍの発行者による信任情報(t_1,t_2,t_3)を抽出する。

【０２７９】ステップ３３０３）　制御部２１０は、改札者装置３００の制御部３１０にｍと(t_1,t_2,t_3)を転送する。

【０２８０】ステップ３３０４）　制御部３１０は、以下の手順により(s_1,s_2)を生成する。

【０２８１】（ａ）　番号生成部３３０により番号r_Eの払出しを受ける。

【０２８２】（ｂ）　r_Eを格納部３４０の番号集合R_Eに追加する。

【０２８３】（ｃ）　$(s_1,s_2)=(H(PkE),r_E)$を生成する。ここで、PkEは制御部３１０が保持する検証鍵である。

【０２８４】ステップ３３０５）　制御部３１０は、利用者装置２００の制御部２１０に(s_1,s_2)を転送する。

【０２８５】ステップ３３０６）　制御部２１０は、耐タンパ装置２８０の制御部２３０に(s_1,s_2)と消費対象チケットのハッシュH(m)を転送する。

【０２８６】ステップ３３０７）　耐タンパ装置２８０の制御部２３０は、格納部２７０に格納されたC_Uについて、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１０に処理の失敗を通知する。

【０２８７】$\exists c_2((H(m),c_2) \in C_U)$　　（１７）

式（１７）は、譲渡対象チケットｍに対応するトークン$(H(m),c_2)$が耐タンパ装置２８０の格納部２７０に格納されていることの検証である。

【０２８８】ステップ３３０８）　耐タンパ装置２８０の制御部２３０は、署名部２５０が備えるS_{PkU}と利用者装置２００の制御部２１０が保持する検証鍵PkU，PkA及び、鍵証明書$(PkU,S_{PkA}(PkU))$を用い、トークン交換形式$e=(e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8)$を得る。ここで、eの各要素は以下の値を採る。

【０２８９】

$e_1=H(m)$

$e_2=c_2$

$e_3=s_1$

$e_4=s_2$

$e_5=S_{PkU}(H(m) \| c_2 \| s_1 \| s_2)$

$e_6=PkU$

$e_7=S_{PkA}(PkU)$

$e_8=PkA$

ステップ３３０９）　耐タンパ装置２８０の制御部２３０は、s_2が正であるなら、C_Uから$(H(m),c_2)$を削除する。

【０２９０】ステップ３３１０）　耐タンパ装置２８０の制御部２３０は、制御部２１０にｅを転送する。

【０２９１】ステップ３３１１）　制御部２１０は、改札者装置３００の制御部３１０にｅを転送する。

【０２９２】ステップ３３１２）　認証部３２０を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、利用者装置２００の制御部２１０の処理の中断を通知する。

【０２９３】

$$e_3=H(PkE) \qquad (18)$$

$$e_4 \in R_E \qquad (19)$$

$$V_{e6}(e_1 \| e_2 \| e_3 \| e_4,e_5)=1 \qquad (20)$$

$V_{e8}(e_6,e_7)=1$ （２１）

$H(e_8) \in t_1$ （２２）

$V_{t3}(t_1,t_2)=1$ （２３）

$e_2=H(t_3)$ （２４）

式（１８）及び式（１９）は、セッション情報の正当性の検証である。この検証により、当該改札者装置３００以外に宛られたトークン交換形式の利用や、トークン交換形式の再利用などによる不正を防止する。

【０２９４】式（２０）は、トークン交換形式に対する署名の正当性の検証であり、この検証により、トークン交換形式の改竄を防止する。

【０２９５】式（２１）は、当該署名者の鍵証明書の検証である。また、式（２２）は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式（２３）は、該信任情報の正当性の検証であり、式（２４）は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンパ性が保証されていることを確認する。

【０２９６】ステップ３３１３） 改札者装置３００の制御部３１０は、格納部３４０のR_Eから$e_4(=r_E)$を削除する。

【０２９７】ステップ３３１４） 制御部３１０は、以下の式が成立することを検証する。検証に失敗した場合は、処理に中断を利用者装置２００の制御部２１０に通知する。検証に成功した場合は、mに対応するサービスをチケットの消費者に提供する。

【０２９８】

$e_1=H(m)$ （２５）

$e_2 \in I_E$ （２６）

式（２５）及び式（２６）は、転送されたトークンが対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、消費されたチケットが有効であることを確認する。

【０２９９】制御部３１において発行者情報がデータごとに管理されている場合は、式（２６）は$e_2 \in I_E(m)$となる。

【０３００】（４） チケット提示の場合：チケット提示は、（３）チケット消費の場合の処理において、以下の変更を加えることにより可能になる。

【０３０１】・ステップ３３０４の（ｃ）において、$(s_1,s_2)=(H(PkE),-r_E)$を生成する。

【０３０２】・ステップ３３１２において、式（１９）を$-e_4 \in R_E$ とする。

【０３０３】以上の変更により、s_2が負数となるため、ステップ３３０９において、C_Uからの削除は行われない。即ち、送信側の利用者装置２に有効なチケットを残したまま、当該利用者装置２が該提示時点で有効なチケットを保持していることを検証すること、即ち、チケットの検札が可能となる。

【０３０４】なお、以上のそれぞれの場合（１）～（４）の説明において、転送されたトークン交換形式は、明示的に保存しなかった。しかしながら、該トークン交換形式の格納部２２０などに保存しておき、該トークン交換形式及びmの受信の際に共に受信したトークン交換形式の履歴をmの送信の際に共に送信することにより、耐タンパ装置２８が破られるなどして不正行為（二重使用）が発見された場合に、不正が行われた装置を特定することが可能となる。

【０３０５】（５）チケットの還流

次に、改札者が消費、提示を受けたチケットを発行者に還流し、対価を発行者が改札者に支払う場合について説明する。このようにすることによって、改札や検札を行なった改札者に対して、二重請求を防ぎつつ手数料などの対価を提供することが可能になる。

【０３０６】発行者装置１００は、トークン交換形式eを格納する手段（格納部１６０）と、還流されるチケットに対応するデータmおよび信任情報(t_1,t_2,t_3)を保持または入手する手段をさらに有するものとする。

【０３０７】以下は、改札者装置３００が消費または提示を受けたチケットを発行者装置１００に還流するチケット還流処理の流れである。

【０３０８】ステップ５５０１）改札者装置３００は、消費または提示を受けたチケットに対応するトークン交換形式eを発行者装置１００に転送する。

【０３０９】ステップ５５０２）発行者装置１００の制御部１１０は、eに含まれるe_2について、$e_2=H(PkI)$であることを検証する。検証に失敗した場合、その旨を通知するとともに以後の処理を中断する。これは、eが自身が発行したチケットに対応するものであるかどうかの検証である。

【０３１０】ステップ５５０３）制御部１１０は、eについて式（２０－２２）が成立することを検証する。ただし、信任情報(t_1,t_2,t_3)が信頼できない経路（改札者など）から入手された場合、式（２３、２４）もあわせて検証する。ただし、式（２４）の検証では、t_3の代わりにPkIを用いる。検証に失敗した場合、その旨を通知するとともに以後の処理を中断する。これは、eが正当な流通経路を介して流通されたことの検証である。

【０３１１】ステップ５５０４）制御部１１０は、e_4が正である場合、eに含まれるe_3について、e_3がt_1によって信任された第３者によって、耐タンパ性を保証されていないことを検証する。これは、eにより有効なトークンが格納されていない（消費により正しく権利が消滅した）ことの検証である。

【０３１２】ステップ５５０５）制御部１１０は、eを格納部１６０に格納する。もし、すでにeが格納部１６０に格納済であった場合、その旨を通知するとともに以後の処理を中断する。

【０３１３】ステップ５５０６）発行者は、還流されたチケットに応じた対価を改札者に提供する。

【０３１４】（６）回数券

次に、トークンおよびトークン交換形式に、度数ないし個数に相当する数値情報を追加し、対応するチケットの「枚数」とし、回数券を実現する例について説明する。

【０３１５】これにより、同一内容、同一発行者のチケットが複数発行されても正しく扱えるようにするとともに、複数の同一トークンを効率的に送信できるようになる。

【０３１６】具体的には、上述した実施例における以下の変更により上記の回数券は実現される。

【０３１７】・トークンに度数情報c_3を追加する。

【０３１８】・トークン交換形式に度数情報e_nを追加する。

【０３１９】・チケット発行において、トークン生成時（S1102）に発行するチケット枚数をnとして指定する。

【０３２０】・チケット譲渡／消費において、（S2207, S3306）の際に譲渡／消費するチケット枚数をnとして指定する。

【０３２１】・チケット譲渡／消費において、トークン保持の検証時（S2208－S3307）に、度数が充分にあることを検証する。すなわち、$c_1=H(m) \cap c_3 \geq n$が成立する(c_1,c_2,c_3)がC_Uに含まれることを検証する。

【０３２２】・全処理において、トークン交換形式生成時（S1108, S2209, S3308）に、$e_n=n$を追加するとともに、e_5の署名対象にnを追加して連接する$(c_1 \| c_2 \| s_1 \| s_2 \| n$となる。）

・チケット譲渡／消費において、トークン削除時（S2210, S3309：s_2が正の場合）に、$c_3=n$の場合にのみ$(H(m),c_2,c_3)$をC_Uから削除し、$c_3>n$の場合はC_Uの$(H(m),c_2,c_3)$を$(H(m),c_2,c_3-n)$に更新する。

【０３２３】・全処理において、トークン交換形式検証時（S1111, S2214, S3312）のe_5による署名検証（式（3），式（１０），式（20））の検証対象にe_nを追加して連接する$(e_1 \| e_2 \| e_3 \| e_4 \| e_n$となる）。

【０３２４】・チケット発行／譲渡において、トークン格納時（S1113、S2216）に$e_1=c_1, e_2=c_2$が共に成立するトークン$(c_1,,c_2,c_3)$がC_Uにすでに存在する場合、C_U中の該トークン$(c_1,,c_2,c_3)$を$(c_1,,c_2,c_3+e_n)$に更新する。

【０３２５】・チケット消費／還流において、サービスや対価の提供はさらにe_nにも応じて行なう。

【０３２６】（７）　再送制御

次に、転送路の不意の切断など、異常が発生した後にトークンの再送を（複製を防ぎつつ）可能にするための処理について説明する。

【０３２７】具体的には、各手順に、以下の処理を追加する。

【０３２８】・制御部１１０、２３０は、トークン交換形式の生成（S1108, S2209－S3308）の際に、生成したトークン交換形式eを保持する。

【０３２９】・制御部２１０、３１０は、受領通知（S1115,S2218における正常終了、S3314におけるサービスの提供）の際に、（チケット送り側の）制御部１１０、２１０に(s_1,s_2)を通知する。

【０３３０】・制御部１１０、２１０は、上記受領通知を受けたら、(s_1,s_2)に対応するトークン交換形式を消去する。

【０３３１】また、再送の際は、各手順において以下の変更を行なう。

【０３３２】・セッション情報生成（S1106, S2205, S3304）の際に、（新親にセッション情報を生成するのではなく）格納部２２０、３４０に格納されているセッション情報(s_1,s_2)を用いる。

【０３３３】・トークン交換形式生成に関連する処理（S1108,S2208-2210、S3307－3309）において、制御部１１０、２１０が$(e_3=s_1) \cap (e_4=s_2)$が成立するeを保持している場合、これらの処理によりeを生成せず、保持しているeを用いて以後の処理を行なう。

【０３３４】（８）発行のバリエーション

チケット発行とは、論理的にはチケット（トークン）生成+チケット譲渡と考えることができるため、たとえば以下のような手順によりチケット譲渡処理を用いてチケットの発行を行なうことが可能である。ただし、チケット発行よりもチケット譲渡のほうが検証処理が多いため、両手順とも本来のチケット発行と比較して処理量は増大する。

【０３３５】（８－１）自己証明書の利用

下記のようにすることにより、制御部２３０によるトークン交換形式の検証は、チケット発行（S1111）とチケット譲渡（S2214）とで異なる。これを（S2214における検証で）一本化し、制御部２３０の実装コストを軽減する。

【０３３６】制御部１１０は、自己による鍵証明書$(PkI, Sp_{kI}(PkI))$を保持する。以下、チケット発行の手順において、以下の変更を加えることにより、チケット発行の場合とチケット譲渡の場合とで、（受信側）制御部２３０における処理が同一化可能となる。

【０３３７】・信任情報生成部150による信任情報生成（S1103）の際に、自らのフィンガープリントH(PkI)を、発行者による信任対象t_1に含ませる。

【０３３８】・トークン交換形式e生成（S1108）の際に、$e_7=Sp_{kI}(PkI), e_8=PkI$とする。

【０３３９】・トークン交換形式eの検証（S1111）の際に、式（1）-(4)のかわりに式（8－14）を用いる。（ただし、UbはUに置き換える）

（８－２）利用者装置によるチケット発行

下記の通り、利用者装置に、自己を発行者とするトークン（のみ）を生成する機能を持たせることにより、利用

者装置によるチケット発行が可能になる。

【０３４０】また、以下の手順により、利用者装置２００によるチケット発行を行なうことが可能になる。ただし、以下の説明においてはデータmは生成済であるとする。

【０３４１】・制御部210は、チケットに対応するデータのハッシュ値H(m)と、信任対象のt_1={H(PkA$_1$),H(PkA$_2$),…,H(PkA$_i$)}を制御部２３０に与える。

【０３４２】・制御部２３０は、保持する検証鍵PkUを用い、格納部２７０に(H(m), H(PkU))を格納する。

【０３４３】・制御部２３０は、署名部２５０を用いてt_2=Sp$_{kU}$(H(PkA$_1$)‖H(PkA$_2$)‖…‖H(PkA$_i$))を生成する。

【０３４４】・制御部２３０は、(t_1,t_2,t_3= PkU)を制御部２１０に返却する。

【０３４５】制御部２１０は(t_1,t_2,t_3)を格納部２２０に格納する。以下、チケット譲渡を行なう。

【０３４６】なお、上記の還流、回数券、再送制御、発行のバリエーションの例は、第１の実施例にも適用可能である。

【０３４７】また、上記の実施例は、図１３～図１６に示す構成に基づいて説明したが、この例に限定されることなく、発行者装置、利用者装置、改札者装置、及び接続装置の各機能をプログラムとして構築し、発行者装置、利用者装置、改札者装置、及び接続装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【０３４８】図２１は、本発明の実施例で説明した記録媒体を使用するコンピュータシステムのハードウェア構成の例を示すブロック図である。本コンピュータシステムは、処理を実行するＣＰＵ５００、プログラムやデータを記憶するメモリ５０１、メモリ５０１またはＣＰＵ５００で使用するプログラムやデータを蓄積する外部記憶装置５０２、データを表示するディスプレイ５０３、データまたは命令を入力するキーボード５０４、ネットワークを介して他のコンピュータシステム等と通信を行うための通信処理装置５０５から構成される。上記プログラムはメモリ５０１又は外部記憶装置５０２にインストールされＣＰＵ５００により実行される。

【０３４９】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【０３５０】

【発明の効果】上述のように、本発明によれば、発行者が信用する経路のみを介してトークンを移送し、利用者や改札者が当該発行者を特定することにより、データに対応するトークンについて、該トークン内のトークン発行者情報が示す発行者以外により、該トークンをトークン格納部に新規に格納することを防止すると共に、該トークンが転送の過程において複数のトークン格納部に複製されることを防止する。

【０３５１】また、トークンを原本情報とし、特定の発行者により発行されたトークンを伴うデータのみを原本とすることにより、当該発行者が原本数を制限することが可能となる。

【０３５２】また、ネットワーク上に存在する情報の識別子（ＵＲＬなど）をデータとして用いることにより、該情報の複製不能かつ譲渡可能なアクセス権を実現することができる。

【０３５３】また、権利内容を記述したチケットないし、当該チケットの識別子を本発明におけるデータとして用い、有効なトークンを伴うチケットのみを有効なチケットとし、利用者や改札者がそれ以外を無効なチケットとして拒否することにより、チケット自体を耐タンパ装置に格納することなしに、チケットの不正な行使（二重使用や不当な複製など）を防止することが可能となる。

【０３５４】また、プログラムを本発明におけるデータして用い、特定の発行者により発行されたトークンを該プログラムの実行ライセンスとし、プログラムの実行器は、該トークンを伴うプログラム以外の実行を拒否することにより、不当に複製された該プログラムの実行を防止することが可能となる。

【０３５５】また、音楽データや画像データを本発明におけるデータとして用い、特定の発行者により発行されたトークンを該データの鑑賞権として用い、データの表示器もしくは、再生器は該トークンを伴うデータ以外の表示や再生を拒否することにより、不当に複製された該データの鑑賞を防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例における原理を説明するための図である。

【図２】本発明の第１の実施例のデータ蓄積システムの全体構成図である。

【図３】本発明の第１の実施例のデータ蓄積システムの発行者装置の構成図である。

【図４】本発明の第１の実施例のデータ蓄積システムの利用者装置の構成図である。

【図５】本発明の第１の実施例のデータ蓄積システムの改札者装置の構成図である。

【図６】本発明の第１の実施例のデータ蓄積システムの接続装置の構成図である。

【図７】本発明の第１の実施例のデータ蓄積システムのチケット発行処理の　シーケンスチャートである。

【図８】本発明の第１の実施例のデータ蓄積システムのチケット譲渡処理の　シーケンスチャート（その１）である。

【図９】本発明の第１の実施例のデータ蓄積システムのチケット譲渡処理の　シーケンスチャート（その２）で

ある。

【図１０】本発明の第１の実施例のデータ蓄積システムのチケット消費処理の　シーケンスチャートである。

【図１１】本発明の第２の実施例の原理構成図である。

【図１２】本発明の第２の実施例の原本流通システムにおけるデータ蓄積システムの構成図である。

【図１３】本発明の第２の実施例の原本データ流通システムの発行者装置の構成図である。

【図１４】本発明の第２の実施例の原本データ流通システムの利用者装置の構成図である。

【図１５】本発明の第２の実施例の原本データ流通システムの改札者装置の構成図である。

【図１６】本発明の第２の実施例の原本データ流通システムの接続装置の構成図である。

【図１７】本発明の第２の実施例の原本データ流通システムのチケット発行の場合の動作を示すシーケンスチャートである。

【図１８】本発明の第２の実施例の原本データ流通システムのチケット譲渡の場合の動作を示すシーケンスチャート（その１）である。

【図１９】本発明の第２の実施例の原本データ流通システムのチケット譲渡の場合の動作を示すシーケンスチャート（その２）である。

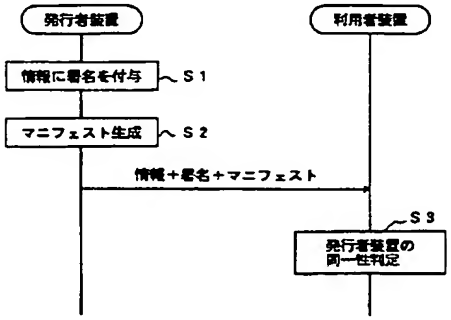
【図２０】本発明の第２の実施例の原本データ流通システムのチケット消費の場合の動作を示すシーケンスチャートである。

【図２１】コンピュータの構成図である。

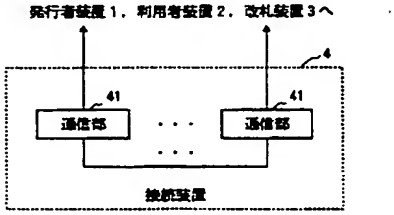
【符号の説明】

１、１００　発行者装置
２、２００　利用者装置
３、３００　改札者装置
４、４００　接続装置
１１、１１０　制御部
１２、１２０　署名部
１３、１３０　データ生成部
１４　マニフェスト生成部
１５、１５０　信任情報生成部
２１、２１０　制御部
２２、２２０　格納部
２３、２３０　制御部
２４、２４０　認証部
２５、２５０　署名部
２６、２６０　番号生成部
２７、２７０　格納部
３１、３１０　制御部
３２、３２０　認証部
３３、３３０　番号生成部
３４、３４０　格納部
４１、４１０　通信部
５０　発行者装置
５１　第１の原本性情報生成手段
５２　第１の原本性情報転送手段
６０　利用者装置
６１　第２の原本性情報転送手段
６２　第１の特定手段
６３　第１の認証手段
６４　格納手段
７０　改札者装置
７１　第２の特定手段
７２　第２の認証手段
７３　データ処理手段
１４０　トークン生成部
５００　ＣＰＵ
５０１　メモリ
５０２　外部記憶装置
５０３　ディスプレイ
５０４　キーボード
５０５　通信処理装置

【図１】

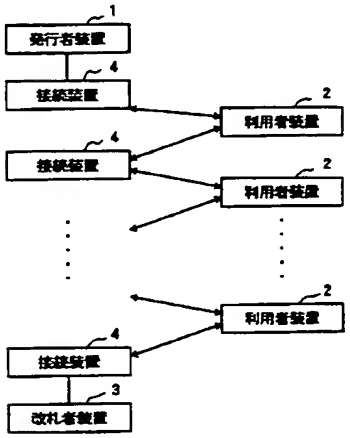


【図６】



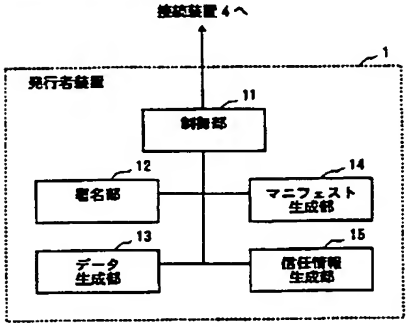
【図２】

本発明の第１の実施例のデータ蓄積システムの全体構成図



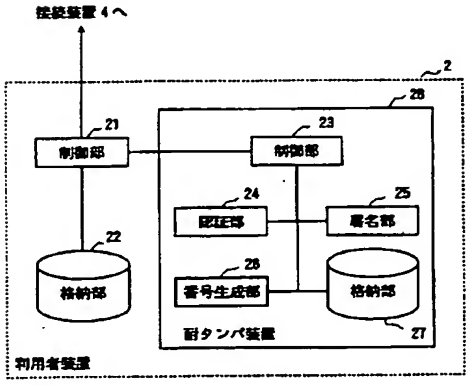
【図３】

本発明の第１の実施例のデータ蓄積システムの発行者装置の構成図



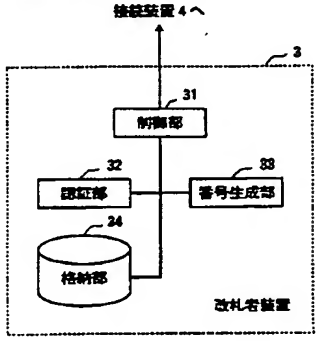
【図４】

本発明の第１の実施例のデータ蓄積システムの利用者装置の構成図



【図５】

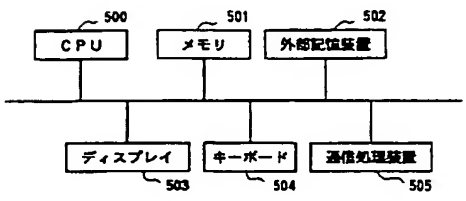
本発明の第１の実施例のデータ蓄積システムの改札者装置の構成図



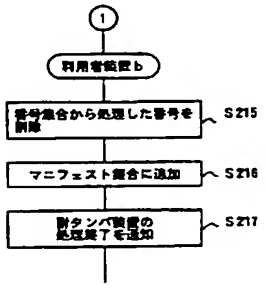
【図９】

【図２１】

コンピュータの構成図

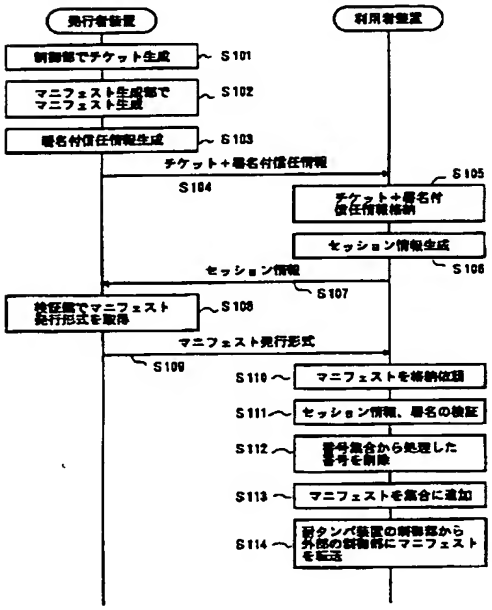


本発明の第１の実施例のデータ蓄積システムのチケット購買処理のシーケンスチャート（その２）



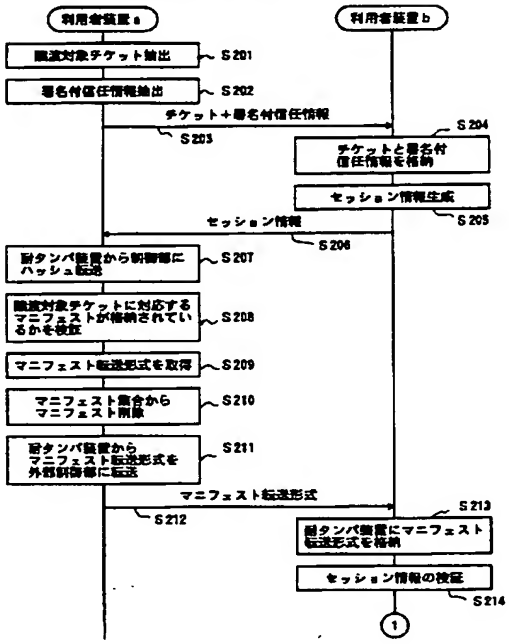
【図７】

本発明の第１の実施例のデータ蓄積システムの
チケット発行処理のシーケンスチャート



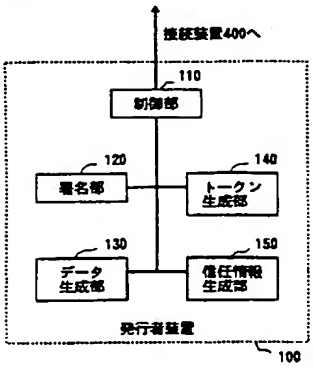
【図８】

本発明の第１の実施例のデータ蓄積システムの
チケット譲渡処理のシーケンスチャート（その１）



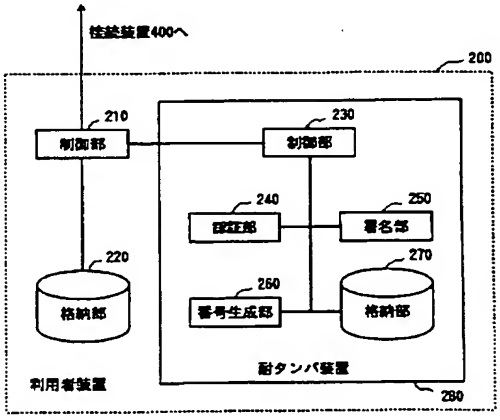
【図１３】

本発明の第２の実施例の原本データ流通システムの
発行者装置の構成図



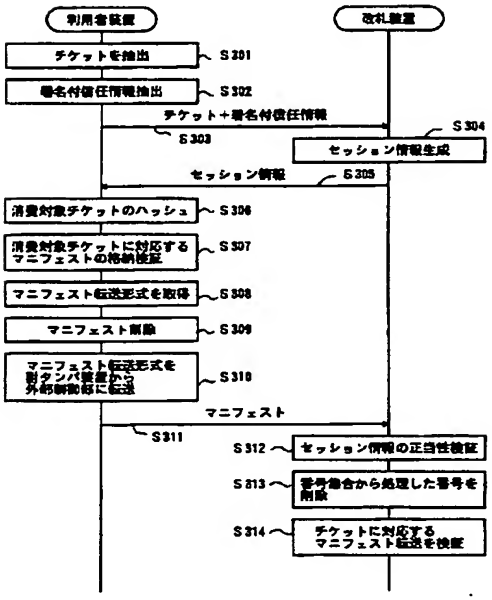
【図１４】

本発明の第２の実施例の原本データ流通システムの
利用者装置の構成図



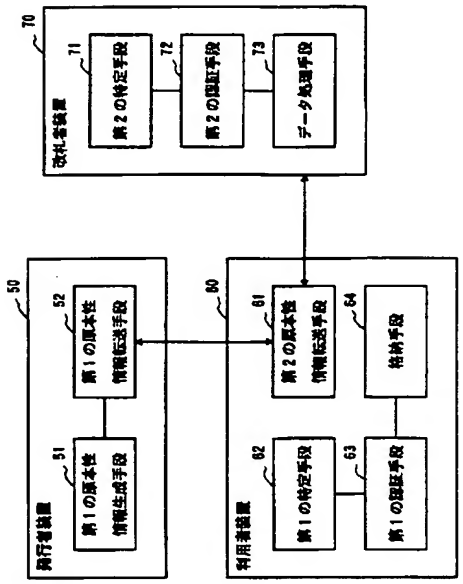
【図１０】

本発明の第１の実施例のデータ蓄積システムの
チケット消費処理のシーケンスチャート



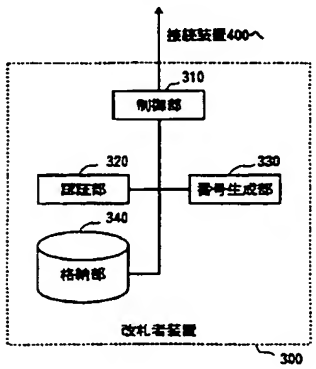
【図１１】

本発明の第２の実施例の原理構成図



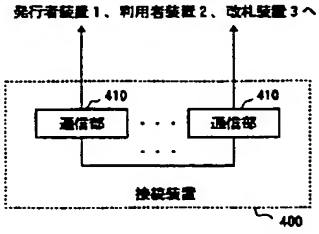
【図１５】

本発明の第２の実施例の原本データ流通システムの
改札者装置の構成図



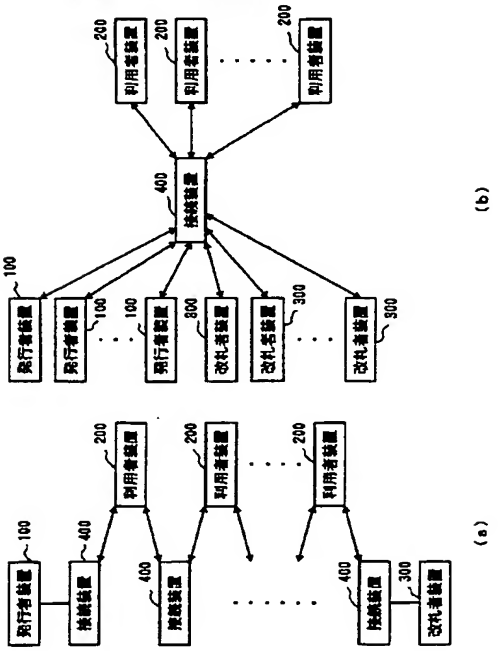
【図１６】

本発明の第２の実施例の原本データ流出システムの
接続装置の構成図



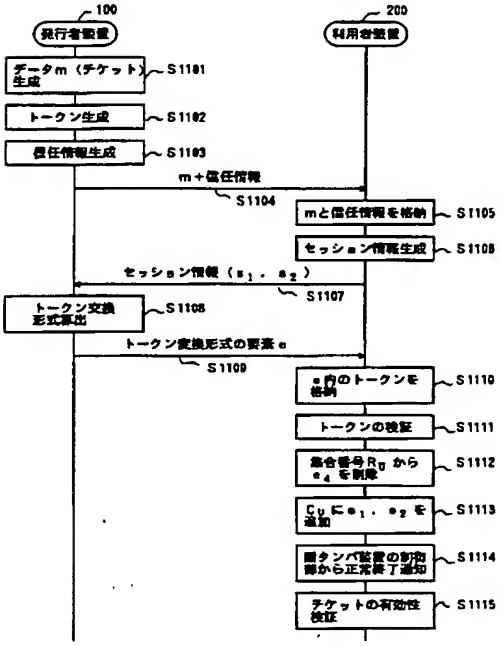
【図１２】

本発明の第２の実施例の原本流通システムにおける
データ蓄積システムの構成図



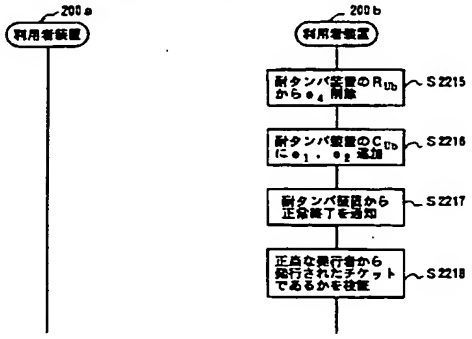
【図１７】

本発明の第２の実施例の原本データ流通システムの
チケット発行の場合の動作を示すシーケンスチャート



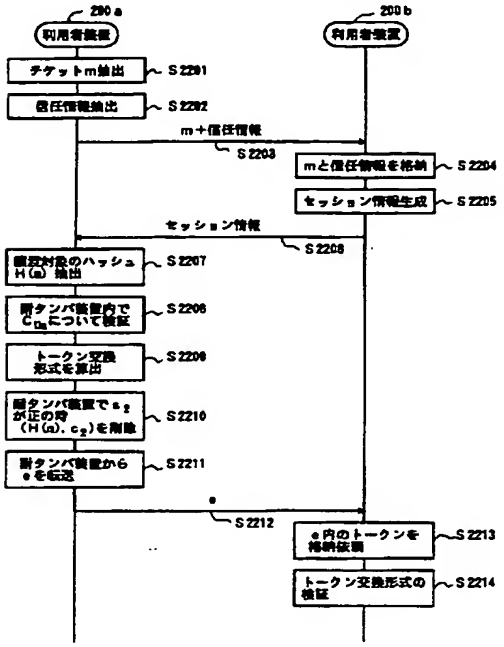
【図１９】

本発明の第２の実施例の原本データ流通システムの
チケット譲渡の場合の動作を示すシーケンスチャート（その2）



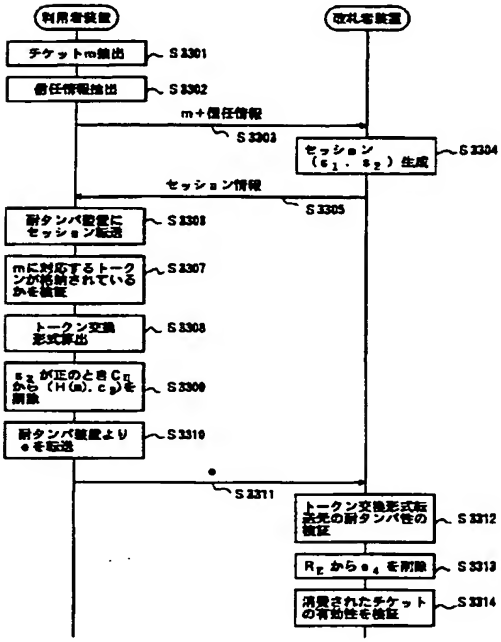
【図１８】

本発明の第２の実施例の原本データ流通システムの
チケット譲渡の場合の動作を示すシーケンスチャート（その1）



【図２０】

本発明の第２の実施例の原本データ流通システムの
チケット消費の場合の動作を示すシーケンスチャート



フロントページの続き

(51)Int.Cl.7	識別記号	FI	テーマコード(参考)
		H04L 9/00	621A

(72)発明者　久野　浩
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　花舘　蔵之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Fターム(参考)　5B017 AA06 BA07 BB02 BB10 CA15 CA16
5B055 BB10 HA02 HA12 HA17 JJ05 KK05
5D044 DE17 DE49 DE50 HL11
5J104 AA09 LA02 LA03 LA06 NA02 NA27 NA42 PA14
9A001 EE03 EE07 JJ51 LL03